Outsourcing: United States Overview

MARK HEAPHY AND JOHN KENNEDY, WIGGIN AND DANA LLP

Law stated as at 01 Jul 2017

Search the Resource ID numbers in blue on Westlaw for more.

A Q&A guide to outsourcing in the United States.

This Q&A guide gives a high level overview of legal and regulatory requirements on different types of outsourcing; commonly used legal structures; procurement processes; formalities required for transferring or leasing assets; data protection issues; customer remedies and protections; contracting parties' remedies; dispute resolution; and the tax issues arising on an outsourcing.

To compare answers across multiple jurisdictions, visit the Outsourcing Country Q&A tool.

This Q&A is part of the multi-jurisdictional guide to outsourcing. For a full list of jurisdictional Q&As, visit www.practicallaw.com/outsourcing-guide.

For the rules relating to transferring employees, visit Transferring employees on an outsourcing in the United States: overview (2-578-7833).

REGULATION AND REQUIREMENTS

NATIONAL REGULATIONS

1. To what extent does national law specifically regulate outsourcing transactions?

US federal laws do not specifically regulate outsourcing transactions. Contract law is generally governed by state law, subject to any applicable federal laws (such as laws relating to intellectual property (IP) rights, immigration, export controls and bankruptcy).

Certain industries such as healthcare, finance and insurance are regulated either on a state or federal level or both. These regulations (and related regulatory guidelines) frequently affect the negotiated content of outsourcing transactions to the extent that the outsourced activities implicate regulatory obligations of the entity purchasing the outsourced services. For example, outsourcing transactions involving entities subject to federal financial laws (such as banking laws) may address certain regulatory compliance obligations of the customer financial entity if the outsourced functions affect the customer's ability to comply with regulatory reporting, audit, privacy and data security requirements.

SECTORAL REGULATIONS

2. What additional regulations may be relevant for the following types of outsourcing?

FINANCIAL SERVICES

Federal and state laws governing the privacy and security of consumer and customer data in the financial services industry frequently affect outsourcing transactions in which customer and consumer data is accessed or processed by outsourcing vendors. Relevant federal agencies overseeing the financial services industry include the:

- Federal Reserve.
- Office of Comptroller of the Currency.
- Federal Deposit Insurance Corporation.
- Financial Regulatory Industry Authority.
- Securities and Exchange Commission.
- Consumer Financial Protection Bureau.

Statutes that may be implicated include the federal Gramm-Leach-Bliley Act and its implementing regulations under state insurance departments and other state financial privacy laws. Federal laws

governing the banking and securities industries may also be relevant where an outsourcing transaction touches upon the financial entity's customer functions or is regulated or subject to specified compliance and audit requirements.

Debt collection activities are regulated on both a state and federal level. Many states impose licensing requirements on debt collectors.

Other statutes that may apply to outsourcing transactions by banks, lenders and other financial services companies, and which require them to meet various disclosure, reporting and anti-money laundering requirements, include the:

- Bank Service Company Act.
- Bank Secrecy Act.
- US Patriot Act.
- Secure and Fair Enforcement Mortgage Licensing Act.

The Federal Trade Commission (FTC) enforces various consumer protection laws which may apply to activities carried out in connection with outsourcing agreements, including the Fair Credit Reporting Act.

BUSINESS PROCESS

Finance and accounting, human resources and procurement outsourcing offerings in the private sector are not generally regulated. However, each specific business process outsourcing offering (including the ones listed above) must each be analysed anew, for example:

- Supplier personnel cannot perform the unauthorised practice of accounting or law in finance and accounting or procurement offerings.
- In a human resources offering, a supplier cannot perform services in violation of applicable employment law.

IT AND CLOUD SERVICES

The internet service provider (ISP) and cloud computing services industry are not significantly regulated in their outsourcing activities except to the extent that a commercial customer may itself be regulated in the activities being outsourced. Transactions with an international footprint which include cross-border transfers of data, software or other technology may need to address certain legal issues related to export, sanctions and embargo requirements. For example, the US regulates the export of certain materials (including certain types of encryption and other technologies) outside of the US under the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR).

The Office of Foreign Assets Control in the US Department of the Treasury oversees the enforcement of certain prohibitions of commerce with blocked individuals and sanctioned countries. The US Bureau of Industry and Security has issued guidelines concerning certain deemed exports of software and controlled information through cloud computing services.

TELECOMMUNICATIONS

There are no regulations specifically governing the outsourcing of telecommunications. However, certain outsourcing arrangements may have to comply with ancillary rules. For example, Federal Communications Commission (FCC) regulations may be relevant, especially in deals involving Consumer Proprietary Network Information (CPNI), which cannot be freely shared among providers. It is also increasingly common for such arrangements to involve data security and network management, which may require regulatory compliance measures under state and federal law.

PUBLIC SECTOR

On both a state and federal level, public contracting in the US is highly regulated and with often material differences from contracting terms in the private sector. For political reasons, large public contracts for outsourcing services are less common than in the private sector. In recent years, there has also been litigation related to certain large public sector outsourcing projects (for example, the litigation between IBM and the State of Indiana in relation to a US$1.3 billion welfare modernisation contract).

OTHER

Personal health information is regulated by the:

- Health Insurance Portability and Accountability Act 1996 (HIPAA).
- Health Information Technology for Economic and Clinical Health Act 2009 (HITECH).

The HIPAA and HITECH regulate both covered entities (such as hospitals, pharmaceutical companies and insurers) and business associates (outsourcing suppliers) with respect to their creation, receipt and transmission of personal health information. Outsourcing vendors that process personal health information received from HIPAA-covered entities must enter into business associate agreements with their customers and are directly subject to certain terms of the HIPAA Privacy Rule and Security Rule.

3. What further legal or regulatory requirements (formal or informal) are there concerning outsourcing in any industry sector?

There is generally not extensive regulation of outsourcing contracts in the US. However, some sectors of the economy, in particular financial services and healthcare, are subject to significant requirements regarding the:

- Safety and soundness of their operations.
- Protection of sensitive personal information of consumers, customers and patients.

As a general rule, the more sensitive the data involved in an outsourcing transaction, the more closely the parties should examine potential state and federal regulations concerning the protection of such data from unauthorised access and use. Such sensitive information may include data financial accounts and records, healthcare data and healthcare payment data, or data involving protected areas such as race, gender, ethnicity and/or sexual orientation.

FINANCIAL SERVICES

Financial institutions are subject to additional regulations. For example, the Office of the Controller of the Currency (OCC) and the Federal Reserve Board (FRB) have issued guidance on how financial institutions should manage risks for third party suppliers. The security rule under the Gramm-Leach-Bliley Act obligates covered

institutions to conduct due diligence on suppliers of outsourcing and cloud services and to engage in oversight of such suppliers.

The Federal Trade Commission has sanctioned mortgage-servicing companies that engage outsourcing suppliers without conducting meaningful due diligence or obtaining basic assurances from suppliers concerning the data security protections for customer data.

The New York State Department of Finance has implemented a new cybersecurity regulation for all entities that must register with and are under the supervision of the Department. Among other things, the new regulation imposes specific requirements on financial entities to conduct appropriate due diligence and obtain certain minimal contractual assurances from vendors, including providers of outsourcing services.

HEALTHCARE

The federal HIPAA and HITECH statutes impose significant obligations on covered entities and on their suppliers who access personal health information, including detailed and specific requirements under the HIPAA privacy and security rules. Outsourcing transactions in this sector must address these requirements to the extent the scope of services touches upon the customer's and the supplier's HIPAA-related obligations. State laws governing healthcare and medical confidentiality should also be consulted.

PUBLIC COMPANIES

Under the Sarbanes-Oxley Act (SOX), public companies in the US must maintain and certify the accuracy of their required public disclosures, including their financials. Accordingly, outsourcing contracts with public company customers typically include undertakings by the supplier to:

- Co-operate with the customer with respect to such disclosures.
- Comply with applicable SOX audit requirements.

4. What requirements (formal or informal) are there for regulatory notification or approval of outsourcing transactions in any industry sector?

There are generally few regulatory notification requirements for entering into or receiving governmental approval of outsourcing transactions in the private sector.

A patchwork of state and local municipal laws impose notice, disclosure and other requirements on outsourcing by state or municipal agencies. These must be consulted on a state and city basis where government agencies are procuring outsourced services.

Under the Security Exchange Act 1934, some publicly traded companies are required to report certain agreements not made in the ordinary course of a company's business. These companies must report the terms of any "material definitive agreement not made in the ordinary course of business" under Item 1.01 of Form 8-K within four business days. Suppliers will often seek to redact pricing and other sensitive terms from such reporting, but the companies themselves ultimately decide what, if anything, is redacted from their submission. A "material definitive agreement" provides for "obligations that are material to and enforceable" against or by the registrant. An agreement is "not made in the ordinary course of business" if it involves either:

- Business not normally conducted by the registrant.
- Subject matter that is identified in items 601(b)(10)(ii)(A) to 601(b)(10)(ii)(D) of Regulation S-K of the Security Exchange Act. This includes "any contract upon which the registrant's business is substantially dependent", and may include
  - continuing contracts to sell a major part of the registrants products or services;
  - franchising or licencing agreements; or
  - agreements to use a patent, formula or trade secret upon which the registrant's business depends.

Generally, notification of financial regulators is not required as a prerequisite to or condition for entering into an outsourcing transaction with a third party vendor. However, some notice obligations may apply, and any financial institution contemplating engaging a third party vendor to carry out regulated functions should consult with its regulatory counsel to determine whether any notifications are required. For example, under the Bank Service Company Act and the Home Owner's Loan Act, covered financial institutions must notify their primary federal regulator within 30 days of entering into an agreement with a third party service provider.

LEGAL STRUCTURES

5. What legal structures are commonly used in an outsourcing?

UMBRELLA MASTER SERVICES AGREEMENT (MSA) AND STATEMENTS OF WORK (SOW)

Description of structure. The predominant structure used in an outsourcing is a Master Services Agreement (MSA). This is an agreement made between a customer and a supplier for the provision of services. Exhibits or schedules are then attached to the MSA to detail general terms applicable to the MSA as a framework. These include (among others):

- Definitions.
- Customer policies.
- The service level methodology.
- Pricing and fees.
- Terms relating to governance.
- Terms relating to customer/supplier competitors.

The actual description of services will be set out in the Statements of Work (SOWs), attached to the MSA.

The parties may also enter into local country agreements for the performance of services in other countries to which different contract terms applicable apply (such as in relation to tax, employment or billing issues).

Advantages and disadvantages. Through executing new SOWs, this structure provides the flexibility to simply and easily add new types or range of work in the future. The disadvantage of this structure is that in larger transactions documentation can be voluminous and negotiations protracted.

ONE-OFF MASTER MSA

Description of structure. A second common structure is an MSA and exhibits or schedules that are narrowly tailored for the initial transaction (including SOWs, actual service levels, specific transition obligations, facilities, reports and so on).

Advantages and disadvantages. While this structure may neatly describe all obligations, it can be difficult to amend when attempting to add a new type or range of work. This is because the original MSA may not have been drafted to accommodate significant expansions or other changes of service types.

MULTI-SOURCING

Description of structure. Customers commonly do not rely on only one supplier. For even the same or very similar types or ranges of work, a customer may award work to multiple suppliers. For example, the customer may employ a champion and challenger model with a primary supplier and a secondary supplier. Customers may also retain one supplier to manage other suppliers for system integration or other offerings.

Advantages and disadvantages. Multi-sourcing allows customers to diversify their risk and enable customers to more readily adapt their ecosystem of suppliers. However, it may be more difficult to have a single point of accountability for the customer, and it may be more difficult for a customer to manage the multiple relationships.

PROCUREMENT PROCESSES

6. What procurement processes are used to select a supplier of outsourced services?

COMPETITIVE BIDDING PROCESS

To gather information, customers often send a request for information (RFI) to suppliers. After obtaining a sufficient amount of information, customers typically send a request for proposal (RFP) with detailed specifics on pricing, performance and other requirements. The customer will then downselect suppliers at various stages of the process, and if successful, the customer will award work to one or more suppliers.

Very often customers engage outside consultants with experience in the customer's industry sector and in outsourcing transactions to oversee and help manage the entire bidding process end-to-end. In some cases, the outside consultants can have significant involvement in:

- Doing diligence on the customer organisation itself.
- Structuring the overall objectives, solution and service delivery design.

Some customers also engage external legal counsel to advise on legal and regulatory questions and, in some cases, to prepare contractual templates which may become part of the RFP package. Depending upon the scope and size of a proposed transaction, the competitive bidding process can range from a few weeks to several months.

SOLE SOURCE BIDDING PROCESS

Customers sometimes negotiate contracts without a competitive bidding process. For example, a customer may have a strong ongoing relationship with an incumbent supplier.

DUE DILIGENCE

Due diligence of suppliers is required for customers who are in regulated industries (such as financial services, insurance, healthcare) and in any event is a best practice across all industries. Due diligence questionnaires, meetings, interviews and even site visits are frequently used in both competitive and single source bidding of projects. Areas of due diligence should include thorough review of supplier's operational and technological capabilities related to the proposed scope of services and, depending on the type of services, also include the following issues:

- Supplier's depth of experience in the full scope of services contemplated.
- Supplier's customer references, industry track record and financial health.
- Supplier's supported technical and operational standards and certifications, as applicable, including data security.
- Supplier's geographic footprint and subcontractor relationships, as applicable.
- Legal diligence (for example, prior regulatory compliance issues or litigation).

TRANSFERRING OR LEASING ASSETS

FORMALITIES FOR TRANSFER

7. What formalities are required to transfer assets on an outsourcing?

IMMOVABLE PROPERTY

Transfers of physical assets and real estate are rare in outsourcing transactions. Immovable property can be transferred through a written agreement. Certain types of immovable property (such as title to land and buildings) are transferred in deeds, which are public records.

IP RIGHTS AND LICENCES

Transfers of IP rights and licences are routine in outsourcing transactions. These rights are conveyed in the outsourcing transaction itself. For example, the outsourcing contract may include licences between the parties for access to their proprietary systems and software as necessary to facilitate the transactions. In transactions where a vendor may be asked to create certain deliverables to be owned by the customer, terms of assignment are included. Generally, vendors tend not to assign any ownership interests in their core IP and technologies as part of a service to the customer. In the US, the parties are not legally required to register such IP licences with the applicable patent, trade mark or copyright offices. Where licences to technology (such as software) may be deemed to include an export of the licensed technology, the parties will typically address in the contract their respective compliance obligations under US export control laws.

MOVABLE PROPERTY

Transfers of movable property are not common in outsourcing transactions. Movable property can be transferred through a written agreement (bill of sale).

KEY CONTRACTS

Where as part of the service solution the vendor will take over the management of certain customer contracts (such as contracts with suppliers or service providers to the customer), the outsourcing contract will address the:

- Nature of the transfer.
- Scope of the assigned rights and obligations.
- Parties' obligations to obtain any required consents.

The assignment or other transfers of key contracts must be in writing and executed by the transferor and transferee. The due diligence review of transferred contracts is typically conducted prior to closing the transaction, and the outsourcing contract frequently addresses the parties' respective obligations for obtaining any needed consents for the transfers.

DATA AND INFORMATION

In most outsourcing engagements, personal information on individuals may be processed and, in some cases transferred across jurisdictional boundaries, as part of the provision of services. However, ownership transfers of such personal information are not typically made in outsourcing relationships.

Other types of data and information may be shared or transferred, and, if ownership is to be transferred, can be assigned by the written agreement of the parties. If the data being transferred is subject to export control laws (encryption technologies), the parties must also address compliance with any applicable export control requirements.

If the data and information is personally identifiable information or protected health information, then transfers may be subject to various US regulations. For example, transfers of personally-identifying information of consumers may be restricted by the terms of prior or existing privacy policies of the transferor. In some cases, the US Federal Trade Commission has intervened to block transfers of customer data in cases where customers were promised that such transfers would not be made without customer consent. Transfers of personally-identifying information of EU data subjects to the US will need to comply with an acceptable transfer mechanism, such as the EU Model Contract data transfer terms or the EU/US Privacy Shield. Transfers and processing of protected health information (PHI) under the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act (collectively, HIPAA) may need to be documented through the execution of business associate agreements where the outsourcing customer is a covered entity under HIPAA or where the transferring entity is a business associate of a HIPAA-covered entity.

FORMALITIES FOR LEASING OR LICENSING

8. What formalities are required to lease or license assets on an outsourcing?

IMMOVABLE PROPERTY

Each party normally deals with its lease of immovable property separately and apart from the outsourcing transaction. In certain circumstances, the supplier may be performing services from the customer's facility, and the outsourcing agreement would address each party's respective obligations in relation to the facility. Where outright transfers of ownership are contemplated as part of the overall transaction, this should be in writing and documented and, as appropriate, recorded in accordance with the applicable state law.

IP RIGHTS AND LICENCES

IP rights and licences are an essential component of an outsourcing transaction. The licences are typically included in the outsourcing agreement itself, and if third parties are implicated, the relevant contracting party must contract with such third party for the applicable licence rights. Transfers of ownership of IP rights (such as copyrighted materials, patented inventions and so on) must be in writing and must be recorded in accordance with the recordation requirements of the applicable government agency (for example, the US Copyright Office for the assignment of copyrights and the US Patent and Trademark office for assignments of patents and trade marks).

MOVABLE PROPERTY

Movable property must also be transferred through written assignments where ownership is being transferred. If property to be transferred is leased by the transferor, written permission of the lessor will likely be required. Similarly, if any moveable property is subject to liens or security interested, written permission to transfer will likely be recorded. Some US states may impose data cleansing requirements on the resale or re-leasing of computer and copying equipment, in order to protect the privacy of individuals whose data may reside on the devices.

KEY CONTRACTS

Temporary assignment of key contracts must be in writing, executed by the parties, and such assignments may require consent and payment of charges to the third parties that are counter-parties to such agreements. The outsourcing agreement will typically address the parties' respective obligations for obtaining such consent and paying such charges, as well as any residual obligations that will remain the party assigning the contract.

DATA AND INFORMATION

See *Question 7, Data and information.*

TRANSFERRING EMPLOYEES ON AN OUTSOURCING

9. Are employees transferred by operation of law?

INITIAL OUTSOURCING

In the US, employees are not transferred by operation of law, and parties have the freedom to contract for rebadging employees from a customer to an incoming supplier. However, many outsourcing transactions in the US have international scope for global customers, and in the EU (and certain other jurisdictions), there can be a transfer by operation of law of employees located in such jurisdictions, for which contracting parties in the US must account.

CHANGE OF SUPPLIER

The parties have the freedom to contract for rebadging employees from an incumbent supplier to an incoming supplier. However, suppliers are typically reluctant to agree to rebadge employees to

their competitors. Accordingly, the outsourcing contract may include specific terms and conditions governing the customer's ability to selectively hire certain employees of the outgoing service provider or may instead prohibit such transfers altogether.

TERMINATION

The parties have the freedom to contract for rebadging employees from an incumbent supplier back to a customer. However, suppliers view their people as important assets and are often unwilling to permit such hiring, except in certain limited circumstances (such as where the supplier is terminating the employment of the affected resources or some hiring is subject to some small percentage cap).

For more information on transferring employees on an outsourcing, including structuring employee arrangements (including any notice, information and consultation obligations) and calculating redundancy pay, see *Transferring employees on an outsourcing in the United States: overview* (2-578-7833).

DATA PROTECTION AND SECRECY

10. What legal or regulatory requirements and issues may arise on an outsourcing concerning data protection?

DATA PROTECTION AND DATA SECURITY

General requirements. The US takes a fragmented and sectoral approach to the law of data protection and data security. There is an assortment of state and federal laws on the topic, many of which are focused specifically on the industry sector (such as healthcare, financial services, insurance, telecommunications, and education). In general, these laws establish:

- The requirements governing the protection of the privacy and security of personally-identifying information of individuals whose data may be stored and processed by a company.
- Consumer rights based on notice of and consent to data collection practices.
- Consumer rights regarding access to and correction of inaccurate data about them.

Depending upon the industry sector of the outsourcing customer, the outsourcing contract may address specific obligations of the outsourcing service provider concerning the protection of personally-identifying information of individuals whose data may be accessed or processed under the agreement. For example, such obligations can include:

- Placing restrictions on the use and transfer of personal information.
- Requiring co-operation from the customer in connection with customer requests to access and correct or delete their data.
- Measures designed to insure that the data processing under the contract complies with the customer's specific regulatory obligations regarding personal data.
- Acknowledging the customer's ownership of its customer data and data derived from such customer data.

Security requirements. Data security terms have become an increasingly significant part of outsourcing contract negotiations.

As with data protection and privacy, the legal structure in the US is fragmented, and there is no single or uniform set of statutory or regulatory requirements for the security of consumer personal data. Specific requirements tend to depend on the industry sector, for example:

- The financial services sector is subject to the Gramm-Leach Bliley Act and its implementation by various state and federal regulators (state insurance departments and, at the federal level, the Federal Reserve, Office of Comptroller of the Currency and the Securities and Exchange Commission).
- The healthcare sector is subject to the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act and the related regulations that govern the privacy and security of protected health information.

For companies subject to the Federal Trade Commission's jurisdiction under Section 5 of the Federal Trade Commission Act, the Commission has built up a body of federal "common law" based on more than ten years of consent decrees and enforcement actions direct at businesses whose approach to data security is arguably "deceptive" or "unfair". Guidelines for businesses and case summaries issued by the Commission, such as "Start with Security" have become an informal benchmark of what generally constitutes reasonable or negligent data security practices in the private sector.

Various state laws also regulate the security of personally identifiable information in general commerce (as well as in the health and financial sectors), but these laws are not uniform. For example, some states have statutes requiring companies to maintain written information security policies and to meet certain minimum data security measures in their handling of personal data.

Some states, such as New York, are beginning to implement their own industry-specific requirements and guidelines for cybersecurity preparedness on the part of regulated companies. New York's new cybersecurity regulation is overseen by the State's Department of Finance and prescribes a variety of minimum practices for protecting cybersecurity of customer data and related information systems. These include due diligence and contract-related requirements for managing cybersecurity when using outside vendors, such as outsourcing service providers.

Mechanisms to ensure compliance. The enforcement of data security requirements in the private sector generally falls to regulatory agencies that oversee sector-specific requirements. For example, federal financial regulators oversee compliance with data security obligations of the entities they regulate (federal banking and securities regulators) by conducting industry examinations and investigations.

State financial regulators oversee the enforcement of state-issued data security regulations (for example, the New York State Department of Finance oversees compliance with that state's new cybersecurity regulation for financial services companies). State data breach notification laws are generally overseen by state attorneys general.

In both federal and state enforcement activity, companies that run afoul of data security requirements may be subject to investigations, litigation or consent decrees that include injunctive relief and in some cases fines.

Few of the state and federal data security laws include a private right of action allowing individual consumers to sue for damages, although there is substantial litigation in the US based on other theories of relief (breach of contract and negligence).

International standards. Transactions that include transfers of personal data of EU data subjects to the US must address the data transfer requirements under Directive 95/46/EC on data protection (Data Protection Directive) and from May 2018 under Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) in order to meet EU standards for the adequate protection of personal data. Mechanisms for compliant EU to US data transfers include the EU-approved Model Clauses data transfer contract forms and the new EU/US Privacy Shield, which is administered by the US Department of Commerce and enforced by the Federal Trade Commission. The outsourcing contract will typically address the agreed transfer mechanism and related data protection and security standards.

Transfers of personal data in an outsourcing transaction involving the US and Asian countries participating in the APEC trade group may follow the APEC Cross Border Privacy Rules System.

Sanctions for non-compliance. Non-compliance with state or federal data security laws may lead to investigation and enforcement actions by the relevant regulatory authority. Sanctions issues can include voluntary consent decrees that include significant ongoing obligations by subject companies to multiple data security procedures and disclosures. In some cases, the underlying statute may authorise the imposition of fines, penalties and/or restitution to affected consumers.

In general, the costs of responding to data breaches in the US can be costly, even when the victim company is not subject to regulatory fines or litigation settlement costs. Therefore, the allocation of data breach-related costs is almost always a significant item for negotiation.

BANKING SECRECY

General requirements. The Bank Secrecy Act (BSA) is the primary US anti-money laundering (AML) law and has been amended to include certain provisions of Title III of the USA PATRIOT Act to detect, deter and disrupt terrorist financing networks. The BSA imposes numerous compliance, monitoring and reporting requirements on covered financial institutions. To the extent that a covered institution's outsourcing agreement with a vendor includes functions that are part of the institution's BSA compliance obligations, it is important for the parties to accurately document these requirements in the contract. Typically, the customer's internal or external banking regulatory counsel are involved in identifying these requirements.

Security requirements. US bank secrecy laws, including the BSA, include numerous requirements concerning confidentiality, security, record-keeping and reporting for data generated in connection with banking transactions and funds transfers. To the extent that a covered institution's outsourcing agreement with a vendor includes functions that are part of the institution's BSA security and confidentiality-related obligations, it is important for the parties to accurately document these requirements in the contract.

Mechanisms to ensure compliance. US federal banking agencies have issued extensive bulletins and guidance to US banking institutions regarding requirements and expectations for overseeing third party vendors who perform outsourced services that support banking functions. These agencies can impose audits and examinations, as well as reporting requirements by covered institutions, to ensure that the applicable bank secrecy regulatory requirements are being properly implemented in the outsourcing relationship. Some banking agencies take the position that they may exercise direct authority over third party vendors that carry out regulated banking functions for US banking institutions.

Sanctions for non-compliance. Violations of US bank secrecy laws can result in significant fines, penalties and injunctive measures affecting a banking institution's conduct of business.

CONFIDENTIALITY OF CUSTOMER DATA

General requirements. Mutual confidentiality clauses are always included in outsourcing agreements and typically address the following items:

- Definition of "confidential information" for both parties. These terms increasingly carve out information that is personally-identifying and subject to data protection and data privacy laws, with the latter data being addressed through the agreement's separate terms directed to the safeguarding of such data.
- Restrictions on use and disclosure of a party's confidential information except as required to perform contractual obligations under the agreement and any other specific permitted uses agreed to by the parties in writing.
- Standard exceptions to the definition of confidential information, such as:
  - publicly available information;
  - information obtained by a party without violation of the agreement's terms or any other applicable confidentiality obligation pertaining to such information; and
  - information independently developed by a party without use of or reference to Confidential Information provided by the other party.
- Terms providing for the return or destruction of confidential information received by a party upon written notice or termination/expiration of the agreement.
- Terms for notice and co-operation between the parties in the event that one party receives a court order, regulatory request or discovery request for confidential information from the other party.

Security requirements. Standard terms obligate the parties to protect the security and confidentiality of the other party's confidential information using measures that are at least as stringent as the measures that the party uses to protect its own similar information, but in any event not less than reasonable security measures under the circumstance. For information subject to data protection and privacy laws, see above, *Data protection and data security.*

Mechanisms to ensure compliance. Agreements typically include obligations to notify a party if its confidential information that is in the possession of the other party has been compromised or accessed. Contractual remedies for breach are available, as well as injunctive relief where compromise of confidential information poses the risk of irreparable harm to the party that owns the information.

Some agreements may also include audit requirements, which allow one party to confirm that the other party is in compliance with the agreement's terms regarding the protection of confidential information.

International standards. Confidentiality terms are typically enforced under the governing law specified in the agreement. To the extent that an international standard may apply to the level of security to be applied to certain information, these would be normally be specified in the agreement.

Sanctions for non-compliance. Agreements commonly provide for significant or unlimited damages for a party's breach of its confidentiality obligations to the other, as well as for termination rights for the aggrieved party.

SERVICE SPECIFICATION AND LEVELS

11. How is the service specification typically drawn up and by whom?

The services are generally described in a statement of work intended to form part of the overall agreement. A statement of work may be initially drafted by either party, and the parties co-operate to finalise the statement of work throughout the negotiation process. If the customer retains a third-party consultant, the third-party consultant is typically very involved in the process of drafting and negotiating a statement of work.

12. How are the service levels and the service credits scheme typically dealt with in the contract documentation?

The specific service levels are generally set out in a service level matrix associated with a particular scope of work, and the service level mechanics are addressed in a service level methodology (which is often attached as an exhibit or schedule to a MSA). Service levels themselves are objective metrics reported at agreed intervals (most commonly on a monthly basis). Service levels are based on either:

- The historic performance of a customer or an incumbent provider.
- Data collected during a baselining of the supplier's actual performance (a six month baselining period).

Failure to meet a service level is typically associated with a service level credit, which is based on a percentage of the charges or at risk amount (most commonly 8% to 12% of monthly charges). Contracts often contain a process for suppliers to earn back credits through subsequent good performance.

FLEXIBILITY IN VOLUMES PURCHASED

13. What level of flexibility is allowed to adjust the volumes customers purchase?

Parties often negotiate very specific volume models for the needs of a customer. In a resource-based model, the parties adjust pricing based on:

- Additional resource charges.
- Reduced resource credits.

The parties may also have a trigger for pricing renegotiation if volumes are outside of a certain percentage band (20%) of a volume baseline. For insourcing and/or resourcing of the services, customers will typically pay termination for convenience fees for volume adjustments. Some outsourcing contracts may also allow for negotiating major volume adjustments and re-pricing upon the occurrence of extraordinary events (such as major regulatory changes affecting the customer, major market events and so on) that affect the business requirements of the customer.

CHARGING METHODS AND KEY TERMS

14. What charging methods are commonly used on an outsourcing?

RESOURCE-BASED CHARGES

In a resource-based pricing scheme, a pre-agreed fixed monthly fee applies for a volume baseline, which can be adjusted with additional resource charges (ARCs) and reduced resource credits (RRCs), and customers pay the supplier more or less depending on the ARCs and RRCs. The resource unit for computing the above can be based on full-time equivalent employees (FTEs) or a transaction-based measurement unit. Parties will often agree to have a baselining period to determine if the volume baseline and number of resource units (FTEs) are accurate. Outside of the ARCs and RRCs volume band, parties generally agree to a trigger for re-pricing.

TIME AND MATERIALS

Parties often contract for suppliers to provide resources on a time-and-materials basis (that is, the rates for personnel may be on a rate card). This arrangement may supplement a resource-based fee structure, where project work can be added to the base services being provided. This structure provides flexibility in relation to the amount and scope of work to be performed.

FIXED PRICE

If the scope of work is well defined and not subject to large variations, the parties may contract on a pre-agreed fixed fee covering the entire scope of work. Nonetheless, the contract will contain certain assumptions underlying the fixed price terms and often provides a change procedure to address increases or decreases in the scope of services during the term of the agreement.

COST PLUS

Some or all charges under an outsourcing contract may be structured on a "cost plus" basis, consisting of an agreed overall cost for delivery of the services plus an across-the-board mark-up of the base cost to provide for the service provider's agreed overall return or profit on the transaction.

15. What other key terms are used in relation to costs, including auditing and benchmarking mechanisms?

Other key terms related to costs include the following:

- Financial audits to verify the accuracy of the charges billed.
- Benchmarking to verify the cost-competitiveness of the charges.

- Inflation clauses to update the pricing based on inflation indexes or foreign exchange rate clauses to manage the risk of currency fluctuations.
- Change control provisions to account for changes in scope of the agreed services or the addition of new services not within the original transaction scope.
- Gain share provisions for sharing cost savings achieved over the course of the agreement.
- Caps on disputed fees (for example, where the customer can withhold a maximum of one or two month cap before other measures are triggered, such as dispute resolution and/or creation of an escrow account into which disputed fees must be paid until the matter is resolved).

CUSTOMER REMEDIES AND PROTECTIONS

16. If the supplier fails to perform its obligations, what remedies and relief are available to the customer under general law?

If the supplier fails to perform its obligations, the customer can file an action against the supplier for breach of contract and claim damages (for example, expenses for substitute services).

Certain defined breaches and material breaches may give rise under the contract terms to the customer's right to terminate for cause. If a dispute involves claims of IP infringement or violation of confidentiality terms, the injured party can seek temporary injunctive relief based upon a showing of irreparable harm. However, instances of such injunctive relief being awarded are generally rare in the outsourcing industry.

17. What customer protections are typically included in the contract documentation to supplement relief available under general law?

Additional contract remedies may include the following:

- Level credits to the customer based on the supplier's failure to achieve one or more service levels.
- Milestone credits associated with the supplier missing one or more key milestone dates for an initial transition prior to the provision of steady-state services.
- Customer termination rights for the supplier's failure to meet its performance obligations (material breach of the agreement or a certain percentage of unexcused service level misses over a protracted time period).
- The customer's negotiated right to withhold disputed charges (subject to a cap on such amount).
- The customer's ability to remove the supplier's subcontractors and/or personnel on a lawful and reasonable basis.
- Step-in rights exercisable by the customer in the event of supplier's failure to perform critical services (though step-in rights can often prove difficult to implement in practice), and a defined step-out when the service provider demonstrates its ability to resume providing such critical services.
- Requirements for the supplier to procure liability insurance from a third party insurer.
- Parental financial guarantee if the entity performing services is thinly capitalised.
- Termination assistance services requiring supplier to assist the customer in performing the services itself or through a third party at termination.
- Governance escalation provisions, which may also include mediation or binding arbitration provisions.
- Indemnification provisions by supplier of customer.
- Warranty provisions by supplier of customer.

WARRANTIES AND INDEMNITIES

18. What warranties and/or indemnities are typically included in the contract documentation?

The warranties and indemnities in a contract often vary significantly depending on the applicable Master Services Agreement and the scope of services.

Customers typically request the following warranties:

- Authorisation to sign and execute the agreement.
- That performance of the services will be performed in a professional and workmanlike manner, in some cases with reference to particular industry standards.
- That services and/or deliverables will meet agreed performance requirements and specifications in the agreement.
- IP non-infringement of all deliverables and supplier materials to be accessed or used by the customer.
- No malicious and/or disabling code in deliverables or supplier systems that will be used or accessed by the customer.
- Compliance with laws.

Customers typically request the following indemnities against third-party claims:

- Any IP infringement of third party rights caused by the deliverables and supplier materials.
- Bodily injury to or death of individuals and tangible property damage.
- Supplier's misuse or misappropriation of confidential information.
- Supplier's compliance with supplier laws.
- Supplier's non-payment of tax obligations allocated to the supplier under the contract.
- Supplier's responsibility for the employment of its personnel.

To the extent applicable, suppliers generally require all of the warranties and indemnities to be made mutual, will resist subjective references to "industry standards" or "best practices" and will be unwilling to indemnify against simple breaches or performance-based claims (such as mistakes, which are inevitable with any human process), particularly where the indemnities carry unlimited liability.

19. What limitations are imposed by national or local law on fitness for purpose and quality of service, or similar warranties?

Most states in the US impose implied warranties for fitness for purpose and merchantability. In practice, these warranties are often excluded in a disclaimer included at the end of the representations and warranties provision in a contract.

20. What other provisions may be included in the contractual documentation to protect the customer or supplier regarding any liabilities and obligations arising in connection with outsourcing?

Outsourcing agreements include a mutual limitation of liability provision and mutual indemnities. The limitation of liability clause typically:

- Places a cap on the parties' exposure to direct damages (subject to certain negotiated exceptions).
- Excludes liability for certain business losses (such as a drop in stock price due to a data breach).
- Excludes indirect, special, consequential and punitive damages.

21. What types of insurance are available in your jurisdiction concerning outsourcing, and to what extent are they available?

As a standard, suppliers generally maintain the following types of insurance:

- Workers' compensation.
- Employer's liability.
- Commercial general liability.
- Automobile liability insurance.
- Fidelity/crime insurance.
- Errors and omissions liability (professional liability) insurance.
- Umbrella liability insurance.

Increasingly, customers ask for insurance for cybersecurity-related liabilities, including for data breaches. While some suppliers may maintain separate insurance for this, cybersecurity insurance is generally written more for customers than suppliers, and for a supplier, errors and omissions liability insurance covers at least some types of cybersecurity claims envisioned by customers.

Common terms relating to the supplier's insurance obligations include:

- Notification requirements concerning changes to the supplier's required insurance coverage.
- The naming of the customer as an additional insured.

TERM AND NOTICE PERIOD

22. Does national or local law impose any maximum or minimum term on an outsourcing? If so, can the parties vary this by agreement?

The parties are free to contract for the term of an outsourcing agreement. Terms of three to seven years are typical, and it is common for customers to have the option to unilaterally extend the term for a short duration (one year) at the existing terms in effect (including subject to inflation, foreign exchange and the other pricing provisions).

23. Does national or local law regulate the length of notice period required (maximum or minimum)? If so, can the parties vary this by agreement?

Parties are free to contract for notice periods.

TERMINATION AND TERMINATION CONSEQUENCES

EVENTS JUSTIFYING TERMINATION

24. What events justify termination of an outsourcing without giving rise to a claim in damages against the terminating party?

MATERIAL BREACH

Typically, customers can terminate an agreement for a material breach of the agreement to the extent that the supplier fails to remedy the breach within 30 days (or other such agreed period) of receiving notice of the breach.

INSOLVENCY EVENTS

Customers generally have the contractual right to terminate an agreement based on the insolvency or bankruptcy of a supplier, though this right may be limited in practice by bankruptcy law. The notice period for a termination for bankruptcy (60 days) is usually longer than for termination for cause and shorter than termination for convenience.

TERMINATION FOR CONVENIENCE

Customers almost always have the right to terminate an agreement for convenience, in whole or in part. The notice period for a termination for convenience is usually much longer than other termination rights (180 days), and the period varies depending on the specifics of the transaction. Termination for convenience is typically associated with termination fees payable to the supplier, which may include:

- Unamortised investments.
- Wind-down costs (for redeploying personnel or assets).
- Break fee as compensation for unrealised profit due to the early termination.

SUPPLIER TERMINATION FOR NON-PAYMENT

The supplier typically has the right to terminate for non-payment by the customer of undisputed fees, and the notice and remedy period is usually shorter than a material breach termination right (ten days).

25. In what circumstances can the parties exclude or agree additional termination rights?

The parties are free to agree to exclude standard termination rights or agree to additional termination rights. Customers often request additional termination rights, which may include the following:

- Change of control (of supplier or customer).
- Supplier's failure to change pricing terms following extreme benchmarking findings.
- Material adverse events affecting either the supplier or the customer (such as regulatory action prohibiting use of the supplier, material changes in the customer's business and so on).

- Other termination for cause rights (such as rights related to the service levels or at risk amount, for example, defined "chronic" failures of the supplier to achieve critical service levels).

These additional termination rights often vary depending on the specifics of the transaction and the priorities of the customer. Termination fees (if any) for each termination right also are frequently negotiated.

26. What remedies are available to the contracting parties?

In outsourcing agreements, parties may file suit for direct damages for breach of contract, or in certain cases, seek injunctions or other equitable remedies. A customer may request the following as additional contract remedies:

- Service level credits for supplier failures to meet agreed service levels.
- Termination rights for specified transition milestone failures by supplier.
- Termination rights by Statements of Work in whole or in part.
- Termination rights for defined financial events affecting the supplier which are indicative of impending insolvency or bankruptcy.
- Step-in rights for supplier's failure to provide critical services.
- Third party benchmarking rights.

Meanwhile, suppliers are generally concerned about getting paid, and they may request a cap on the amount of charges which may be held in dispute (two months).

IP RIGHTS AND KNOW-HOW POST-TERMINATION

27. What, if any, implied rights are there for the supplier to continue to use licensed IP rights post-termination? To what extent can the parties exclude or include these by agreement?

Licence rights are meticulously negotiated in outsourcing transactions, including disclaimers of implied licences. Licences can run both ways, for example:

- The supplier can grant a non-exclusive licence to the customer to use supplier-provided software or systems.
- The customer can grant a non-exclusive licence to the supplier to the extent the provision of services requires supplier to access or use proprietary customer materials.

Licences typically terminate on termination of the agreement (subject to any period of exit services to the customer) and are not deemed to survive by implied continuing licence grants. In drafting such terms, suppliers are not typically awarded any licence rights to customer's IP (including software), data or confidential information post-termination.

28. To what extent can the customer gain access to the supplier's know-how post-termination and what use can it make of it?

Contracts frequently provide for a period of termination assistance during which the supplier may provide certain knowledge transfer services to the customer to help effect a smooth exit and transition. Customers may also retain copies of the specific operating manual or other written operating procedures used by the parties. In addition, parties often add a mutual residuals clause for the use of know-how retained in the unaided memories of each party's employees. However, these rights are generally subject to the confidentiality and IP ownership provisions of the agreement. As part of termination assistance, suppliers support the transition to another supplier or internally within customer with knowledge transfer activities and other related responsibilities. Suppliers also generally make commercially available products and software available on standard terms post-termination.

LIABILITY, EXCLUSIONS AND CAPS

29. What liability can be excluded?

In the US, sophisticated parties dealing at arm's length generally have the freedom to contract for liability caps and exclusions of certain types of liability (such as indirect damages, lost profits). However, certain types of damages cannot be limited (for example, intentional wrongdoing). Furthermore, under state law, there may be additional types of damages which cannot be capped in the applicable state because the exclusions may be deemed to violate public policy.

30. Are the parties free to agree a cap on liability and, if desirable, a cap on indemnities? If so, how is this usually fixed?

Provided the damages can be limited under the law of the applicable state (*see Question 29*), parties are free to agree to caps on liability, including indemnities. Limitations of liability are often subject to extensive negotiation, with factors under consideration including the:

- Expected length of the contract term.
- Nature of potential anticipated losses as a result of a party's breach.
- Parties' respective abilities to control for their risk.

Typical results from such negotiations may include the following:

- Consequential damages, lost profits and unanticipated savings are typically excluded as compensable losses under all theories of liability, including breach of contract and tort.
- For recurring services, direct damages are commonly capped at the last 12 months of fees (excluding taxes and reimbursable expenses) or some other formula that provides a multiple of some agreed period of fixed recurring costs.
- The above limits generally will not apply for claims of intentional wrongdoing, gross negligence (with an element of recklessness) and certain indemnities that the parties agree may be excluded or limited.

DISPUTE RESOLUTION

31. What are the main methods of dispute resolution used?

A typical dispute resolution provision will include escalation procedures within certain defined time periods. If the dispute is

not resolved during the course of such escalations, which typically culminate at the level of the parties' senior management, a dispute resolution provision typically permits either party to:

- File an action in the applicable courts.
- Invoke a binding arbitration procedure.

In some cases, the parties may agree for certain types of disputes (such as disputes related to confidentiality or IP) to not be subject to the escalation procedures and/or binding arbitration, and in such case, the parties are permitted to immediately file an action.

In some cases, the parties may negotiate "fast track" dispute escalation procedures for certain types of disputes, such as disputed payments to the supplier. Procedures for termination assistance are often negotiated in substantial detail, including the requirement for an agreed termination assistance plan, and this level of planning helps mitigate disputes during the sensitive termination assistance period.

TAX

32. What are the main tax issues that arise on an outsourcing?

TRANSFERS OF ASSETS TO THE SUPPLIER

Assets are not frequently transferred to the supplier in outsourcing transactions (*see Question 7*). If assets are transferred to a supplier, the supplier may be responsible for state and/or local sales or use taxes on the purchase or lease of such assets, and if ownership of assets are transferred to supplier for less than fair market value, then such may constitute additional revenue for supplier. Each party is generally responsible for taxes imposed on its respective assets.

TRANSFERS OF EMPLOYEES TO THE SUPPLIER

When employees are rebadged by a supplier (and become the supplier's employees), the is then supplier responsible for paying the applicable withholding taxes, including any federal, state and/or local income taxes and federal employment and unemployment taxes.

VAT OR SALES TAX

The US does not impose any federal VAT. However, VAT may be applicable for services delivered outside of the US.

On a federal level, the US does not have a sales tax. However, certain state and local entities in the US levy a sales tax on outsourcing services, and customers generally agree to reimburse suppliers for any sales taxes levied on the services.

SERVICE TAXES

This is as stated above with respect to a sales tax on the services (*see above, VAT or sales tax*).

STAMP DUTY

On a federal level, the US does not have a stamp tax.

CORPORATION TAX

Each party is generally responsible for taxes imposed on its income.

OTHER TAX ISSUES

When scope outside of the US is contemplated for a customer, the parties often agree to allocate responsibility for withholding taxes on certain cross-border payments and seek to minimise any such taxes.

ONLINE RESOURCES

US CODE

W *www.gpo.gov/fdsys/browse/collectionUScode.action?collectionCode=USCODE*

Description. Contains available text of the US Code.

CODE OF FEDERAL REGULATIONS

W *www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR*

Description. Contains available text of the Code of Federal Regulations.

CONTRIBUTOR PROFILES

MARK HEAPHY, PARTNER
Wiggin and Dana LLP

T +1 203 498 4356

F +1 203 782 2889

E *mheaphy@wiggin.com*

W *www.wiggin.com*

Professional qualifications. Connecticut, US

Areas of practice. Outsourcing and technology; financial services; healthcare; insurance; life-sciences; manufacturing; telecommunications and utilities.

Non-professional qualifications. JD, University of Virginia School of Law, 1996; MA, Yale University, 1993; BA, College of William & Mary, Phi Beta Kappa, 1990

Recent transactions

- Helped clients to structure, negotiate and document domestic, near-shore and off-shore, commercial relationships related to complex, global, outsourcing strategies in North and South America, Europe, Asia, the Middle East and Africa.
- Worked on hundreds of sole-sourced and competitively-bid sourcing transactions throughout the world, including business-process and information technology outsourcing arrangements, software licensing, support and distribution transactions, technology development and systems integration agreements, joint ventures, strategic alliances and cross-border technology transfers.

JOHN KENNEDY, PARTNER

Wiggin and Dana LLP

T +1 203 363 7640

F +1 203 782 2889

E *jkennedy@wiggin.com*

W *www.wiggin.com*

Professional qualifications. US

Areas of practice. IT; data privacy and security; IP and e-commerce; outsourcing, software development and licensing, e-commerce transactions, technology transfer and intellectual property-intensive M&A, divestitures, joint ventures and restructurings.

Non-professional qualifications. Received JD from Columbia Law School; William Rainey Harper Fellow at the University of Chicago, MA in English and American Literature; graduated magna cum laude from Carleton College.

Recent transactions

- Negotiated complex IT outsourcing services agreements involving cloud computing, IT infrastructure and software procurement, systems integration, software development and maintenance, voice and data services and disaster recovery and business continuity.
- Negotiated business process outsourcing (BPO) agreements for call centres and customer support services, finance and accounting services, HR administration, enterprise procurement services, government passport and visa services, research and development services and supply chain management. His work in this area includes advising clients on all stages of the contract process, including RFP preparation and evaluation, vendor diligence, negotiation of definitive agreements and ongoing advice concerning governance, dispute management and amendments.
- Represented clients in connection with risk and compliance assessments of data privacy policies and practices, data breach preparedness and response, regulatory investigations of data practices, behavioural advertising campaigns and "privacy by design" analyses of products and services in social media and mobile e-commerce, corporate information governance programs, international data transfers and compliance with US state and federal data privacy and information security laws.

Professional associations/memberships. Recently elected to The American Law Institute, the leading independent organisation in the US producing scholarly work to clarify, modernise, and otherwise improve the law.

Publications. Author of numerous articles on privacy and data security and since 2000 has co-chaired Practicing Law Institute's Annual Privacy and Data Security Law Institute. Bloomberg BNA recently published *Privacy & Data Security Practice Portfolio Series, Cybersecurity and Privacy in Business Transactions: Managing Data Risk in Deals*, March 2015.

03-18