Outsourcing: United States Overview

by Mark Heaphy and Tamia Simonis, Wiggin and Dana LLP

Country Q&A | Law stated as at 01-Dec-2022 | United States

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; supply chain compliance; specification, service levels and escalation; flexibility in volumes purchased; charging methods; customer remedies and protections; warranties and indemnities; term and notice period; termination and its consequences; liability, exclusions and caps; dispute resolution; and the tax issues arising on an outsourcing.

Regulation and Industry 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 outsourcing 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?

Sector-specific Regulations

IT and cloud services. The internet service provider 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 relevant legal issues related to privacy and data security as well as 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.

Telecoms. There are no regulations specifically governing the outsourcing of telecommunications. However, certain outsourcing arrangements may have to comply with ancillary rules. For example, the Federal Communications Commission (FCC) regulations may be relevant, especially in deals involving Consumer Proprietary Network Information, 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.

The Telephone Consumer Protection Act 1991 regulates telephone solicitations and automated calling, and it provides a private right of action for consumers to file lawsuits. The FCC has also established a national "do-not-call" registry pursuant to the law and other privacy regulations for businesses subject to FCC regulation.

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 still be analysed at an operational level, for example:

- The supplier (outsourcing service provider) 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.

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 Industry Regulatory Authority.
- Securities and Exchange Commission.
- Consumer Financial Protection Bureau.

Statutes that may be implicated include the federal Gramm-Leach-Bliley Act (GLBA) 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 its other regulated activities and audit requirements.

Debt collection activities are regulated on both a state and federal level, such as through the federal Fair Debt Collection Act and the Fair and Accurate Credit Transactions Act. 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.
- USA Patriot Act and the USA Freedom 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 and Section 5 of the Federal Trade Commission Act.

Certain states impose privacy and security requirements on customers and, in some cases, suppliers. For example, the New York State Department of Financial Services enacted cybersecurity requirements for financial services companies via the State of New York Cybersecurity Regulation (that is, 23 NYCRR 500); and the State of California has implemented privacy protections for consumers in the California Financial Information Privacy Act.

Legal process. Each state separately regulates the practice of law and licenses attorneys. In legal process outsourcing transactions, suppliers cannot engage in the unauthorised practice of law (as defined by applicable State Bar rules of professional ethics).

Knowledge process and other professional services. Other general types of professional services (for example, consulting) are typically not regulated. However, this is not universally true. For example, the American Institute of Certified Public Accountants sets applicable audit standard requirements and professional rules for audit related services.

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. In contracting with the federal government, federal agencies must comply with the Federal Acquisition Regulation, which is a set of principles of the government procurement process, and the Department of Defense must also comply with the Defense Federal Acquisition Regulation Supplement.

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 USD1.3 billion welfare modernisation contract).

Manufacturing. Depending on the scope of services, outsourcing of human resources for a manufacturing entity may raise issues in employment laws and other workplace related laws, including managing employee safety reporting or workers' compensation rules, and suppliers typically follow customer-set processes and directions for these issues. Similarly, certain confidential data of a manufacturer (for example, manufacturers in the defense industry) may be subject to EAR and/or ITAR.

Other. Some outsourcing relationships related to healthcare and healthcare insurance services may involve the processing of regulated data. In the US, certain categories of health information are regulated by various state laws as well as the federal:

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

HIPAA and HITECH regulate certain "covered entities" (such as hospitals, pharmaceutical companies and insurers) and their "business associates" (for example, their suppliers) with respect to their creation, receipt, processing, storage and transmission of Protected Health Information (PHI). Outsourcing vendors that process PHI received from HIPAA-covered entities are directly subject to certain terms of the HIPAA Privacy Rule and Security Rule and must also enter into business associate agreements with those customers.

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.

Other Legal or Regulatory Requirements

Financial services. Financial institutions are subject to additional regulations. For example, the Office of the Controller of the Currency and the Federal Reserve Board have issued guidance on how financial institutions should manage risks for third party suppliers. The security rule under the GLBA obligates covered institutions to conduct due diligence on suppliers of outsourcing and cloud services and to engage in oversight of such suppliers.

The FTC 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.

If an outsourcing supplier undertakes certain regulated activities (for example, certain mortgage, insurance and debt-collection services), the supplier may be required to obtain licences under applicable state law.

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.

Insurance. Under applicable state insurance codes, insurance companies that outsource regulated functions or provide access to regulated data are subject to the core GLBA obligations of due diligence and monitoring/oversight of suppliers. Some states, such as New York and Connecticut, have increased data security and data breach notification requirements on insurers and other financial services companies.

Energy and utilities. The North American Electric Reliability Corporation has issued critical infrastructure protection cybersecurity reliability standards and requirements which owners, operators and users of the "bulk power system" must comply with. This is likely to include customers who operate in the energy industry, and depending on the scope of an outsourcing engagement, it may affect the security requirements of a deal. State agencies (for example, the California Public Utilities Commission) also regulate utilities in their respective states, including with respect to utility rates and practices which affect consumers within the state.

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 parties HIPAA-related obligations. Under HIPAA and HITECH, customers are also required to perform due diligence of the proposed supplier and maintain ongoing control and monitoring over the supplier. 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.

3. What industry sectors require (formally or informally) regulatory notification or approval for outsourcing transactions?

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

Financial Services

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.

Insurance

The insurance industry is regulated on both a state and federal level. Depending on the type of outsourced tasks, the outsourcing supplier may be required to obtain licences from applicable states (for example, third party administrator licences).

Merger Control

See below, *Joint Ventures and Merger Control*.

Joint Ventures and Merger Control

Under the Security Exchange Act, 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. 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 registrant's products or services;
    - franchising or licensing agreements; or
    - agreements to use a patent, formula or trade secret upon which the registrant's business depends.

Structuring the Transaction

> 4. What transaction models are commonly used in an outsourcing in your jurisdiction? What are their respective advantages and disadvantages?

Umbrella Master Services Agreement and Statements of Work

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 data processing, data security and data transfers.
- Terms relating to customer/supplier competitors.

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

The parties may also enter into local country agreements that set out supplementary or alternative contract terms applicable to the performance of services in specific countries (for example, covering specific local tax issues, employment matters or billing requirements).

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

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).

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

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.

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.

Other

Joint ventures, partnerships, captive entities and build operate transfer models for outsourcing are less common, and when used, these structures are highly tailored to the applicable deal.

Atypical deal structures may better suit the parties' commercial goals in a particular case. However, there may be more risks involved in this kind of customised deal (for example, the performance of the services not meeting expectations), and increased costs in negotiating the transaction.

Procuring the Supplier/Service Provider

5. What procurement processes are used to select a service provider or supplier of outsourced services?

Competitive Bidding Process

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

Outsourcing customers often 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 organization 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 request for proposal package. Depending on 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 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

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

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 specific deliverables the customer wishes to own, terms of assignment are included. Generally, vendors will not assign any ownership interests in their core IP and technologies (whether or not developed as part of the customer engagement). 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

In cases 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.

Offshoring

Customers and suppliers generally agree on delivery locations in outsourcing contracts, including delivery locations located offshore. Customers need to ensure there are no restrictions by either contract or under applicable law (for example, export control laws) prohibiting the offshoring of the contemplated scope of services.

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. Transactions that can be characterised as sales or sharing of personal information may trigger additional data privacy compliance obligations, such as under the CCPA/CPRA.

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 (for example, encryption technologies), the parties must also address compliance with any applicable export control requirements.

If the data and information is personally identifiable information or PHI, 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 FTC 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 Standard Contractual Clauses data transfer terms or the EU/US Privacy Shield. Transfers and processing of PHI under HIPAA and HITECH 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

7. 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 needs to 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.

See *Question 7, Data and Information.*

Transferring Employees on an Outsourcing

8. Are employees transferred by operation of law?

For information on transferring employees in an outsourcing transaction in [jurisdiction], including structuring employee arrangements (including any notice, information and consultation obligations) and calculating redundancy pay, see *Country Q&A: Transferring Employees on an Outsourcing in the United States: Overview*.

Data Protection and Secrecy

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

Data Protection and Data Security

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 on 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 ensure that the data processing under the contract complies with the customer's specific regulatory obligations regarding the privacy and security of personal data.
- Acknowledging the customer's ownership of its customer data and data derived from such customer data.

Certain for-profit entities doing business in the state of California must comply with the CCPA/CPRA in connection with the collection of personal information for business purposes. To be subject to the CCPA/CPRA, covered businesses must either:

- Have gross revenues of USD25 million or more.
- Hold personal information of over 100,000 consumers, devices or households.
- Earn over half of its annual revenue selling or sharing consumer's personal data.

The CCPA/CPRA provides rights for consumers, including:

- Right to be informed of and have access to personal information that is collected, sold, shared and disclosed, including information regarding the applicable categories of personal information and sources of such personal information.
- Right to be informed of the business purposes for which, and third parties to whom which, personal information is being collected, sold, shared or disclosed.
- Right to deletion of personal information collected.
- Right to direct a business not to sell or share personal information (opt-out right).
- Opt-in right for sale or sharing of personal information of persons under the age of 16 years.
- Right to delegate a proxy representative.
- Right to equal services and pricing even if CCPA/CPRA rights are exercised.
- Private right of action for data breaches.

Use of processors and sub-processors. Increasingly, some state regulators require customers to include certain data privacy and security related terms in contracts with suppliers (for example, the State of New York Cybersecurity Regulation and California Consumer Protection Act 2018 (CCPA), as amended by the California Privacy Rights Act 2020 (CPRA)). Under the CCPA/CPRA, covered businesses must, among other things, insert provisions in their contracts with suppliers (who receive personal information) to prohibit:

- Selling or sharing the personal information.
- Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
- Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

Liability for breaches of personal data processing requirements (for both the customer and the supplier). While some laws (for example, HIPPA Security Rule) create direct responsibility and liability for breaches of security obligations, most US laws in this area directly regulate the owner or licensee of the data in question (that is, customers and not suppliers), which may include compliance with security requirements and data breach notification requirements.

Transfer of personal data to third countries. Currently, the US does not generally regulate the transfer of personal data to third countries. Sanctioned countries (for example, North Korea and Iran) are an obvious exception to this.

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 GLBA 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, the related regulations that govern the privacy and security of PHI, and applicable state medical privacy laws.

For companies subject to the FTC'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, have implemented their own industry-specific requirements and guidelines for cybersecurity preparedness on the part of regulated companies. New York's cybersecurity regulations prescribe 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 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).

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 and Security

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. Agreements often 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 normally be specified in the agreement.

Sanctions for non-compliance. Agreements commonly provide for significant damages for a party's breach of its confidentiality obligations to the other, as well as for termination rights for the aggrieved party. Increasingly, enhanced damages caps (for example, one and a half or twice the multiple of the basic limitation on a party's liability) are emerging as the dominant market norm. Outsourcing contracts restrict and usually prohibit the recovery of indirect, special, consequential and punitive damages, but these damages are sometimes recoverable for a narrow set of particularly-defined claims, such as breaches of confidentiality (although not usually for data breaches), fraud, gross negligence or wilful misconduct. However, even when consequential damages are recoverable for data breaches, it is typical for agreements to explicitly exclude from the recovery any lost profits, lost revenues, unrealised savings, lost goodwill or share value, reputational injury and similar business losses, which might otherwise be recoverable as consequential damages or, if reasonably foreseeable, as direct damages.

International Standards

Transactions that include transfers of personal data of EU and UK data subjects to the US must address the data transfer requirements under the General Data Protection Regulation (*(EU) 2016/679)* (GDPR) and the GDPR as transposed into the national laws of the UK, in order to meet EU and UK standards for the adequate protection of personal data. The primary mechanism for complying with EU and UK transfers is the EU-approved Standard Contractual Clauses data transfer contract forms (and their counterparts in the UK). There are an increasing set of national privacy and data security regulations from other jurisdictions throughout the world as well (Canada, Switzerland, Australia, India and others) that, where relevant to a particular transaction, must also be addressed in the contractual terms. The outsourcing contract will typically specify in detail 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.

International controls and security standards (such as International Organization for Standardization standards and Society for Worldwide Interbank Financial Telecommunication requirements) may apply to cross-border deals involving banks.

Supply Chain Compliance

10. What (if any) compliance provisions should an outsourcing customer include in the contract?

There are frequently numerous bribery, human trafficking and employee safety and non-discrimination terms flowed down by customers from federal law (such as from the Foreign Corrupt Practices Act) in US only deals. Customers typically include these requirements in the MSA.

Services: Specification, Service Levels and Escalation

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 extensively 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?

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 documented and validated historic performance of a customer or an incumbent provider.
- Data collected during a baselining of the supplier's actual performance (for example, a six-month baselining period starting from the effective date of the agreement).

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.

13. Are there any service escalation mechanisms that are usually included in the contract? How often are these exercised and how effective are they in restoring the services to the required levels?

A well-constructed service level methodology usually functions as an effective management tool for incentivising the proper performance of services. For example, if the supplier fails to meet a pre-agreed service level for an applicable month, the customer may be automatically entitled to receive a service credit off of a subsequent invoice. However, contracts often define some level of repeated, unremedied service level failures over time that constitute unacceptable service, entitling the outsourcing customer to terminate the affected services or, in extreme cases, the relationship as a whole.

Transaction Management

Organisational Structures and Change Management

14. What types of organisational structures are commonly used to govern outsourcing transactions?

Governance involves the practical management of an outsourcing relationship to promote good results and is a critical component in any successful outsourcing transaction.

Good governance typically stems from effective management of day-to-day operations, through designated service provider and customer operations leaders, each empowered to make decisions for their organisation. It also requires executive sponsors and oversight (often through a high-level joint steering committee) with other joint committees or working groups for specific operational or other responsibilities (such as compliance and security). Regular communication and interaction at all levels helps to promote good performance, address issues as or before they arise and forestall difficulties. In practice, effective governance is likely to matter far more than remote contingencies to which the parties may devote greater time and energy. Forms and organisational charts, however sophisticated, have little value unless the parties engage with each other and agree ahead of time how their engagement can be most effective. Talking through the specifics of the arrangement during contractual negotiations is therefore time well spent.

The complexity of the structure varies with the scale of the relationship, but usually, there are multiple layers or tiers, for example:

- At the very top, there are executive sponsors on both sides, which may sometimes be C-level executives (such as the CEO or COO) or, in large companies, a corresponding position in a relevant business unit, that have the necessary authority over their company's engagement.
- The next level below involves executive oversight, often through a joint board or steering committee which may include executive sponsors. This committee should meet regularly (often, quarterly) to review the relationship as a whole, and consider its direction, policy and other overall issues, rather than operational or contentious matters (unless there are issues that require specific escalation, because they are significant and unresolved).

- The next level below comprises the outsourcing's operational management, through the service provider's operations leader and the customer's project manager or representative, who often holds a senior position in the customer's vendor management organisation. These parties may be supported by an operational working group or committee, which may include some their direct reports (for example, persons responsible for billings, budgets, operations, compliance, security and so on).
- Finally, joint working groups or committees, to deal with planning, budgets, changes, compliance, security, special projects or other specific subjects.

It is best practice to conduct periodic reviews of the relationship and to periodically review any specific issues involving compliance and security, or any other matter which permits a fresh look, or (if necessary) re-calibration and to conduct early discussions of any emerging issues, such as technology changes and security threats. Regular management attention helps to encourage expeditious resolution of otherwise potentially contentious issues.

15. What change management models are commonly used to govern outsourcing transactions?

Best Practice for Successful Change Management

Change management is a critical aspect in any successful, long-term outsourcing relationship.

Any additional work carried out by the service provider must be paid for, whether this is through:

- Purely quantitative pricing (for additional full time equivalent hours (FTEs) or chargeable time).
- Formal change orders or provisions to compensate the service provider for net additional costs incurred and services performed for various purposes (for example, in supporting other contractors or accommodating changes in the customer's security or other policies).

Best-practice change management procedures should generally:

- Allow either party to propose changes (not just the customer).
- Specify the contents for any change proposals (for example, in relation to their scope, probable cost, effects on performance and so on).
- Establish a reasonable process for their preparation, review, revision and approval, with reasonable time limits.
- Price any additional work carried out fairly, generally at applicable contract rates or, where no rate applies, at the service provider's then-current standard rates or some other objective basis that is fair to both sides (and not on a "most-favoured" basis).
- Condition the service provider's obligation to perform and the customer's obligation to pay upon written approval of the change.

Some outsourcing agreements distinguish "new services" from other varieties of changes (such as operational, technical, and contractual changes, as well as perhaps other categories). However, differences among the various kinds and categories may be uncertain and debatable. Most changes, however labelled, amend the contract documents in at least some minor particulars, although few changes will amend the master contract text and many routine operational changes have little or no financial impact. From a contractual standpoint, a single change management procedure for all changes can work well, even if different approvals are required for changes with significant financial impact.

Contracts generally provide the service provider with broad discretion to make a variety of operational changes, provided these do not:

- Increase charges and other costs to the customer.
- Adversely affect service quality, including service levels.

Consent for these types of changes is not typically required, although the customer may and should be informed when any emergency changes are made. Good change management procedures permit both customers to request change proposals and for suppliers to offer change proposals on their own initiative. In either case, there should be an agreed form of change proposal that specifically sets out the particulars concerning the scope, timing, cost, impact upon services and service levels, estimated charges, probable effects on other costs, resources required from the customer and other details. There should also be a formal process for the submission, review, and approval or rejection of any proposed changes, which should all be within reasonable time periods. However, change proposals should not remain open indefinitely. Time periods for submissions and approvals should be realistic, reflecting the complexity of the service offering and proposed change, as well as the scale of the relationship.

Making Charges for Changes

Charges for changes are sometimes negotiated on a case-by-case basis, but many customers dislike this approach, fearing uncertainty and the leverage that comes with incumbency. Understandably, service providers want to know what rates and charges will apply to future changes. Nevertheless, there are a few principles common to most change management procedures with respect to pricing:

- There may not be additional charges for services that can be performed with the staff and other resources ordinarily available to support the customer, provided the resources are paid for and the changes do not jeopardize the service level performance, service quality or other responsibilities. However, in all cases this will be subject to the service provider's commitments concerning productivity. For example, in cases where the service provider has committed to rationalise and reduce staff year-on-year, spare capacity to absorb the additional effort may diminish over time.
- Many changes are paid for through normal incremental charges for additional FTEs, transactions, or other chargeable resources and metrics.
- Where no rate or metric exists (for example, in relation to skills or technologies not presently supported for a particular customer) the parties can negotiate on a case-by-case basis, but there is usually an objective standard ("unless otherwise agreed, the service provider's then-current standard rate for such services"). "Most-favoured" pricing of changes will be unacceptable to most service providers. In all cases, customers should understand the general principle that nothing will be for free and the service provider will expect to be compensated for any material, additional efforts.

Flexibility in Volumes Purchased

16. What mechanisms are commonly used to manage adjustments in the volume of services?

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 (for example, 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

17. 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 sometimes 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 will usually provide 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.

18. 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.
- Provisions allocating financial responsibilities between the parties related to currency fluctuations and certain tax assessments, such as withholding taxes.
- Limitations and conditions on the customer's ability to withhold disputed charges (for example, requirement of escrow or expedited resolution when withheld charges exceed a defined threshold).

Customer Remedies and Protections

19. If the service provider 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 (or initiate arbitration or mediation) 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.

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

Contractual rules usually grant customers broad audit rights, subject to reasonable restrictions on frequency, purpose, use of supplier competitors, and so on.

Additional contract remedies may include the following:

- Service 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 specified time period).
- The customer's right to periodic benchmarking of the charges (typically every one to two years, following an initial stabilisation period) against a normalised set of charges by similar providers for a comparable package of services, triggering a customer right to terminate for convenience at a reduced termination fee where the charges exceed the mean of the normalised group by an agreed-upon percentage (automatic price adjustments are unworkable for most providers).
- The customer's 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.
- The customer's right to conduct audits (annually or more frequently) related to the supplier's compliance with certain performance and/or compliance terms of the contract and to remediation of performance or compliance shortfalls identified in the audit.
- Ongoing customer monitoring rights through periodic reports from the supplier, governance meetings and/or real-time monitoring of supplier performance against service levels and key performance indicators.
- 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.

- Financial guarantee from the supplier's parent company 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, with reciprocal indemnification provisions by customer of supplier.
- Warranty provisions by supplier of customer with some, though not typically all, involving reciprocal customer warranties.

Warranties and Indemnities

21. What express 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 MSA and the scope and nature 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 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 certain laws directly applicable to the provider.

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 laws applying to the supplier (as distinct from laws applying to the customer).

- Supplier's acts or omissions (or contractual breaches) resulting in a data breach.
- 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 contractual breach or performance-based claims (such as mistakes, which are inevitable with any human process), particularly where the indemnities carry unlimited liability.

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

Most states in the US impose implied warranties for fitness for purpose and merchantability; however, under the Uniform Commercial Code, such implied statutory warranty requirements generally relate to goods (not services). In practice, these warranties are often excluded in a disclaimer included at the end of the representations and warranties provision in a contract.

23. What types of insurance are available in your jurisdiction concerning outsourcing? Are there any types of insurance required by law?

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.

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 typically requires the outsourcing customer to pay significant termination fees (which are not characterised as penalties) 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. The notice and remedy period is usually shorter than for a material breach termination right (ten days).

Breach of Confidentiality/IP Rights

The supplier typically has the right to terminate for the customers' breach of confidentiality or supplier's IP rights. The notice and remedy period is usually often shorter than for a material breach termination right (ten days).

25. 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). Some customers in highly regulated industries (for example, banking and financial services) also seek termination rights based on court or regulator directives or significant changes in law affecting the viability of the contract.

Exit Arrangements

26. What mechanisms are commonly used to address exit and post-termination transition issues?

In general, US IP law does not create implied rights to use another person's or entity's IP beyond the term of the licence (however, certain exceptions exist under US bankruptcy law). 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 generally are not deemed to survive by implied continuing licence grants. In drafting such terms, neither party is typically awarded any licence rights to the other party's IP (including software), data or confidential information post-termination. However, customers frequently negotiate the right to enter into post-termination licences on pre-agreed terms for specific supplier commercial software packages they may want to continue using following expiration or termination of the agreement.

27. To what extent can the customer (or if applicable, its new service provider) gain access to the service provider'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 agree to support the transition to another supplier or internally within customer with knowledge transfer activities and other related responsibilities. Suppliers will also generally make commercially available products and software available to customers post-termination, on standard terms and charges.

Liability, Exclusions and Caps

28. 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 or lost profits). However, certain types of damages cannot be limited (for example, intentional wrongdoing). Further, 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.

29. 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 32*), parties are free to agree to caps on liability, including indemnities. Limitations of liability are almost always 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.

30. What other provisions may be included in the contract to protect the customer or service provider regarding any liabilities and obligations arising in connection with outsourcing?

As detailed throughout this Q&A, customers and service providers use a variety of contractual terms to define their obligations, allocate responsibilities and confine their respective liabilities. These include, among others, service levels, compliance obligations, confidentiality terms, warranties, disclaimers, indemnification, liability exclusions and damages caps.

One other significant and important mechanism for protecting both parties' interests, however, is to have a clearly-defined scope of the service provider's performance in the applicable Statement of Work, along with an explicit, detailed listing of any technology, personnel and other resources the customer will be expected to provide as part of the arrangement. Clearly defining the scope of the service provider's performance has the following benefits:

- For the service provider: it helps to protect it from unanticipated "scope creep" that can erode its profit margins.
- For the customer: it helps to protect it from unexpected expenditures and/or gaps in service.

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 supplier is then 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.

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 and academic qualifications. Connecticut, US; JD, University of Virginia School of Law, 1996; MA, Yale University, 1993; BA, College of William & Mary, Phi Beta Kappa,1990

Areas of practice. Outsourcing and technology, across all industry sectors.

Experience

- Helped service providers 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 commercial arrangements for business-process and information-technology outsourcing; cloud

migration; robotics, AI and machine learning; software licensing, support and distribution; technology development; systems integration; and cross-border technology transfers.

- **Professional associations/memberships.** Ranked globally and nationally by Chambers and The Legal 500 and regularly honoured in "Best Lawyers in America" for technology law; frequent lecturer on outsourcing, licensing, and privacy issues; served as an adjunct professor at Connecticut's Quinnipiac School of Law for more than a decade.

Tamia M Simonis, Partner

Wiggin and Dana LLP
Professional and academic qualifications. US; JD, Pace University School of Law, graduated valedictorian, summa cum laude; New York University, Stern School of Business; BS in Accounting (CPA program); graduated magna cum laude, University Honor Scholar, Beta Gamma Sigma

Areas of practice. Outsourcing and Technology, across all industry sectors.

Experience

- Assisted global service providers in the negotiation and documentation of hundreds of global complex business process outsourcing (BPO) transactions for call centres and customer support services, finance and accounting services, HR administration, enterprise procurement services, research and development services and supply chain management. Her work in this area includes advising clients on all stages of the contracting process, including RFP preparation and evaluation, vendor diligence, negotiation of definitive agreements and ongoing advice concerning governance, dispute management and amendments.
- Negotiated complex IT outsourcing services agreements involving cloud computing, IT infrastructure and software procurement, robotics, artificial intelligence and machine learning, systems integration, software development and maintenance, and voice and data services.

Professional associations/memberships. Ranked globally and nationally by Chambers and The Legal 500.

END OF DOCUMENT