From *Law360:* Outsourcing Transactions In The Insurance Industry

--By James A. Harvey and Susan Wilson, Alston & Bird LLP

Law360, New York (December 22, 2011, 1:52 PM ET) -- The insurance industry has long been focused on reducing costs and improving operational efficiencies. With the turbulence in today's insurance marketplace, those efforts have been renewed and strengthened, resulting in an increase in outsourcing transactions.

We have also observed an expanded scope of services that would have never before been considered appropriate for sourcing to a third party. In light of this expansion of both volume and scope, this article identifies several of the unique legal issues our insurance industry clients face in today's outsourcing marketplace.

Expanding Scope

Many members of the insurance industry have outsourced information technology (IT) infrastructure and applications development and maintenance services to third parties for a number of years.

Some in the industry have also outsourced significant business processes, such as human resources (whether comprehensively or on a process-by-process basis), finance and accounting, and procurement.

We have recently been engaged in business process transactions involving nontraditional, more value-added services, such as complex claims processing and administration.

In all of these sourcing transactions, insurers have unique legal issues that must be addressed. These issues may be minimized by suppliers in an attempt to speed negotiations and win the customer's business, and insurers may find themselves pressured by time to ignore the subtleties and complications.

While each transaction is unique and presents its own issues, the issues on which we most often invest significant time and energy in insurance industry transactions include (i) responsibility for compliance with laws and (ii) how to adequately protect the privacy and security of sensitive policyholders and other information collected and held by insurers.

We also find that our insurance company clients often need a reminder that insurance holding company systems laws may require their sourcing transaction documents be filed with — and not disapproved by — state insurance regulators.

Compliance with Laws

Given the expanding scope of services that are under consideration in insurance industry sourcing transactions, our clients are encountering increasingly complex compliance issues. Many clients approach this as "winner takes all" and attempt to move the entire compliance obligation to the supplier.

Customers often attempt to require the supplier to be directly responsible for the customer's compliance with the applicable law(s) through a provision that states something to the effect of "Supplier and the Services will be compliant with federal/state law XXX."

Suppliers nearly always resist this position, frequently asserting that direct compliance with any given statute that is applicable to the customer is not within their control or appropriate for the scope of services rendered.

Suppliers, of course, also attempt to swing the issue completely in the other direction. They sometimes seek the safe haven offered by the position that they "do not render legal advice" and "cannot practice law on behalf of the customer."

Suppliers also attempt to offer language, typically found in IT transactions, that they are responsible solely for laws that are "applicable to Supplier's business and the delivery of the Services." From the customer's perspective, particularly in business process outsourcing transactions, this proposed formulation omits critical components of protection.

If a supplier is only responsible for laws applicable to "its business" and the "delivery of the services," then compliance-oriented tasks that arise in the delivery of the services do not fall within the express scope of the supplier's compliance responsibility.

While these positions appear to be accurate when taken entirely out of context, they are often overused by suppliers in an attempt to avoid legitimate responsibility for compliance outcomes that suppliers should assume in sourcing transactions.

The more challenging, but frequently encountered, solution to this issue is the difficult middle ground of assigning responsibility for certain tasks that underlie a particular compliance obligation to either the supplier or the insurance company customer.

If the supplier fails to carry out a particular task that prevents the customer from complying with a given law or regulatory requirement, this middle ground places responsibility for that lack of compliance on the supplier, even though the supplier is not responsible for compliance with the statute or regulation in its entirety.

For example, if the insurer is required to file its quarterly statement within 45 days after the end of a quarter, failure by the supplier to provide all information required for completing the statement should give rise to liability for penalties, fines and damages suffered by the customer for noncompliance.

Identifying, negotiating and drafting this sort of allocation of responsibilities can be an extremely analytical and labor-intensive task, which is often the reason this solution is resisted by customers and suppliers. Suppliers may try to take this formulation too far and require that every single compliance-oriented task be specifically identified by the customer.

Taken to its logical extreme, if a task is not denoted as a compliance obligation, the supplier would have no responsibility from a compliance perspective for that task. This shifts all the burden to the customer, in the context of a services description that is sometimes thousands of lines long.

We recommend that our insurance company clients budget time into their transaction-completion schedules for identifying major compliance needs and negotiating those into the documentation, but that they also take a firm position that the suppliers who elect to operate in the insurance industry must be prepared to accept reasonable responsibility for the associated compliance requirements.

Another difficult area of negotiation involves appropriate remedies for the supplier's failure to meet its compliance obligations. If an insurer fails to comply with applicable laws and regulations, it can be subject to fines and consent orders adversely affecting its operations, imposed by its domiciliary state and other states in which it does business.

Suppliers will often seek to avoid liability for these types of remedies by inserting provisions that exclude consequential and other similar types of damages, which could prevent customers from receiving protection for the most obvious and likely results of noncompliance.

Extreme caution and precision is required when drafting these provisions. This rigor will help prevent what are often regarded as "run-of-the-mill lawyer provisions" "at the back of the document" from denying the customer an opportunity to recover what are reasonably foreseeable, if not likely, damages arising from noncompliance.

Of course, if a task is sufficiently critical, then customers should also consider higher limitations of liability for potential compliance failures.

Privacy and Security

Most insurance companies have terabytes and terabytes of personal data regarding insureds, claimants and employees. Allowing third parties to collect, process, store and transmit this data on behalf of an insurance company is a particularly sensitive undertaking, one that is often accompanied by significant legal and business exposure.

The loss or misuse of this information can have an extensive and expensive impact on an insurance company, both from a monetary perspective and from a reputational perspective.

Depending on the type of information and the exact nature of the insurance products, many participants in the insurance industry have been subject to various aspects of one or both of the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB) for more than a decade.

In the United States, they have also had to deal with the burgeoning list of state breach notification statutes[1] and state-level privacy- and security-related statutory and regulatory requirements.[2]

Those companies with operations in the European Union (EU) also have to address the requirements of the EU Data Directive[3] and member state laws implementing the directive.[4]

Importantly for insurers with EU operations who are engaging in outsourcing transactions, the EU Data Directive imposes significant requirements on the transfer of personally identifiable information outside the EU. These restrictions can have a material impact on the scope of the services outsourced by insurers, the structure of the transaction and the service solutions proposed by suppliers.

While incredibly important and critical to insurance companies, privacy obligations are in many ways a subset of the overall compliance responsibility obligation. Security obligations are a parallel, but separate, critically important issue for members of the insurance industry considering significant outsourcing transactions.

Both HIPAA and GLB require that service providers — or business associates, in HIPAA vernacular — have sufficient security procedures in place.[5] Defining these security procedures is, however, often a difficult task.

Insurance companies are increasingly more sophisticated in their development, maintenance and administration of their security programs; nevertheless, it can be challenging to produce appropriate security requirements for outsourcing suppliers.

Suppliers may attempt to exploit this situation by taking the position that "we only do what we are asked to do with respect to security." This places an extreme premium on the customer's establishment of security requirements; it also raises the legitimate question of whether the supplier should have an underlying standard of care beyond that set forth in the security requirements.

If a supplier does exactly what is required by the security requirements, but is otherwise remiss with the most basic security procedures, many supplier formulations of the risk provisions in the outsourcing agreement would exclude a claim for negligence against the supplier.

Thus, while there is some superficial attraction to the supplier's argument that they should only be required to provide expressly stated security activities, that position should cause insurance companies to focus on a possibly wider and deeper security obligation for which their sourcing suppliers should be liable.[6]

Security breach is, in our experience, the most sensitive issue for both parties in today's insurance industry outsourcing transactions.

Customers are rightly concerned that, because they will be entrusting suppliers with vast repositories of personal data for which the customers have extreme financial, regulatory and reputational risk, suppliers must not allow that information to be accessed and misappropriated by third-party hackers.

Indeed, many outsourcing customers have a knee-jerk reaction and attempt to require suppliers to assume unlimited liability for these types of obligations. Suppliers, of course, argue that they cannot be responsible for every breach and should not serve as an insurance policy against security breach.

As is the case with compliance with laws, today's transactions should find the middle ground, with suppliers assuming responsibility for particular security breach notification and notification-related costs and activities if they have breached their obligations, while still considering whether and to what extent liability should be limited for these events.

Insurance Holding Company Systems Requirements

All 50 of the U.S. states have adopted by law or regulation some version of the National Association of Insurance Commissioner's model Insurance Holding Company System Regulatory Act (Model Act).

Under such laws and regulations, an insurance company is required to file agreements between itself and any affiliate in its holding company system that meets certain criteria. The agreement must be filed with the insurer's domiciliary state insurance regulator and generally not disapproved by such regulator within the 30 days following the filing.

When an insurance company is part of a larger organization, including a holding company and perhaps multiple licensed insurance entities, there is a high likelihood that operations are already combined in some manner to achieve economies of scale.

For example, an insurance holding company might have multiple single-state HMO entities established to enable compliance with state laws regarding providers and other matters, but it might also have one data and accounting center that performs operational functions on a shared services basis.

An outsourcing transaction will likely be, and may even need to be, negotiated on the same consolidated basis. Not only does this follow the current operational structure of the insurance organization, but it also allows for collective bargaining strength by the insurance customer vis-a-vis the supplier, as well as ongoing cost efficiencies and transactional efficiency in completing the deal.

A threshold question for an insurer entering into an outsourcing transaction, however, will be whether to include all of the various licensed entities as parties to the outsourcing agreement, or only the holding company or shared service company.

The answer will depend on factors unique to each situation, but frequently the answer is to keep the documentation simple and include only the holding or shared service company. The agreement can be drafted to make clear that the supplier's services will be for the benefit of all other applicable affiliates, with the fees and costs paid by the holding or shared service company allocated to the participating affiliates.

If the outsourcing documents include multiple insurers as parties, they will almost certainly need to be filed with the applicable domiciliary regulators. If the outsourcing documents include only the holding or shared service company, however, the documents may also be of a type that requires filing.

For example, the Model Act, and most state-adopted versions, requires that all management agreements, service contracts and cost-sharing arrangements be filed, regardless of size.

Consequently, we recommend to our insurance company clients that, at the outset of structuring an outsourcing transaction, they take two actions in this regard: (i) review the organization's existing intercompany management and services agreements to determine if such agreements already allow for the outsourcing transaction, and (ii) if not, allow time in the transaction completion schedule to file the outsourcing documents and obtain regulatory clearance where necessary.

Conclusion

Outsourcing transactions are complex to structure, negotiate and document, particularly for customers operating in a regulated industry like insurance. This is becoming increasingly true as insurers outsource more significant parts of their core operations.

This article discusses briefly a few of the more difficult issues. There are many other considerations unique to the insurance industry, such as whether the supplier needs statutory accounting systems and expertise, and how to ensure that the insurer can comply with requirements to maintain its books and records in its licensed jurisdictions and provide regulatory examiners with access to outsourced books and records.

Given the increase in the number of insurance industry outsourcing transactions and the increasing complexity of the tasks that are outsourced, there are many critical considerations for any insurance company engaging in a material outsourcing transaction.

Jim Harvey is a partner in Alston & Bird's intellectual property and technology transactions group. Susan Wilson is a partner and co-chairwoman of the corporate transactions and securities group. Both are based in the firm's Atlanta office.

[1] Currently 46 states and the District of Columbia have enacted data breach notification statutes. Most statutes require entities holding personal data to notify affected individuals in their state if the personal data is accessed without authorization. Many states also require entities to notify authorities, such as the state's attorney general, in the event of a data breach. See, e.g. Cal. Civ. Code § 1798.82; N.Y. Gen. Bus. Law §899-aa.

[2] See, e.g., Massachusetts Data Protection Law (201 CMR 17.00); Nevada Revised Statutes § 603A.010 et seq.

[3] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the processing of personal data and on the free movement of such data.

[4] See, e.g., German Federal Data Protection Act (BDSG); UK Data Protection Act 1998.

[5] See 16 CFR 313.14.4(d) (GLB service provider requirements) and 42 USC 17931 (HIPAA business associate requirements).

[6] As is the case with compliance with laws, the risk provisions including limitations of liability, exceptions to limitations of liability, and exclusions of consequential damages and other types of damages are critical to the overall resolution of this issue.