

Holding a Bank's Technology Service Providers Accountable

By Kevin J. Funnell

Federal banking regulators expect that a financial institution that outsources technology services to a third party vendor will have contractual remedies that are adequate to protect the institution, in the event that the vendor is negligent or fails to adequately perform its services for the institution. The Federal Financial Institutions Examination Council's Booklet "Outsourcing Technology Services,"¹ which provides guidance to bank examiners and management on evaluating the risks involved with managing outsourced technology services, contains the following advice to institutions and bank examiners on contractual provisions that address the indemnification responsibilities of vendors and that limit the liability of the vendor.

***Indemnification.** Indemnification provisions should require the service provider to hold the financial institution harmless from liability for the negligence of the service provider. Legal counsel should review these provisions to ensure the institution will not be held liable for claims arising as a result of the negligence of the service provider.*

***Limitation of Liability.** Some service provider standard contracts may contain clauses limiting the amount of liability that can be incurred by the service provider. If the institution is considering such a contract, management should assess whether the damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the service provider's failure to perform its obligations.*

The federal banking agencies' guidance to the institutions they supervise, such as that provided by the Office of the Comptroller of the Currency in Bulletin 2001-47 on "Third Party Relationships,"² echoes these requirements. In the Bulletin, the OCC states that it favors indemnification provisions that require each party to indemnify the other for damages and third party claims that result from the negligence of the "indemnifying" party, so that the bank is not liable to third parties for the failures of the service provider.

In an ideal world, a technology service provider would agree to be fully accountable, to the bank and to third parties, for the results of its own negligence and for its failure to perform its services in accordance with the terms of its written agreement with the institution. Unfortunately, I have yet to encounter a major provider of technology products or services who is willing to provide such broad protection.

SERVICE LEVEL AGREEMENTS

Most well-considered technology services agreements contain "service level agreements" (SLAs), pursuant to which the provider agrees to meet certain service levels. For example, a service provider who provides services through an Internet web site might agree that the web site will be fully operational 24 hours a day, seven days a week. A vendor who provides data processing services for a bank would generally agree to be available to

receive the data properly and timely transmitted by the bank within agreed upon business hours and to process the data within certain timeframes and in a certain format. The failure to meet SLAs can cause the bank its own direct losses (for example, the inability to complete trading transactions for its account) and can also expose the bank to claims by any affected customers (for example, customers using online banking services who are unable to complete transactions). Even if the bank may effectively limit its own legal liability to its customers and other third parties through limitation and disclaimer provisions in its customer and other agreements, the bank can still be exposed to damage to its reputation (“reputational risk”).

If the service is a new one for the bank, its personnel may not have sufficient experience in setting SLAs for the service. If the bank’s due diligence does not give it adequate access to the expectation of other banks that use the service, then the parties may agree to establish a monitoring period at the outset of the agreement. After a period (for example 6 months) the parties will agree to establish SLAs and remedies for failure to meet the same. To give some teeth to such a delayed setting of SLAs, the bank should have the right to terminate the agreement without penalty if satisfactory SLA provisions are not agreed upon within a certain period of time.

Banks have every right to demand that a servicer provider be accountable for its failure to meet SLAs, particularly where the failure is more than an isolated occurrence. As a senior executive with Verisign conceded in an article published earlier this year in *The Wall Street Journal*³, “Customers are asking for liability clauses. If we screw up and they suffer some kind of losses, we may have some kind of liability,’ she says, subject to certain limits.” There, of course, is the “rub.” What are the “limits” that the service provider will insist upon and that the bank should accept? Some attorneys advise that these issues are “always open to negotiation.” I would agree, up to a point. The level of exposure that a service provider may be willing to take is affected by a number of factors, but one of the critical factors is the size and importance of the bank to the service provider. All other factors being equal, a smaller customer whose agreement is not likely to be a major revenue producer for the provider is less likely to be in a position to negotiate as favorable terms as a larger bank with a bigger budget for the service. That is not a fact of life confined to the banking business.

Another important factor in the successful negotiation of meaningful remedies for breaches of SLAs is the willingness of the bank to take, and hold, a firm position on the need for such remedies. If the bank has done appropriate due diligence, a service provider who has made it to the stage of contract negotiations is likely to be a provider whose services and pricing are deemed by the bank to be preferable to those of its competitors. Often, bank personnel will have made an emotional investment in the selection of the service provider, and may be reluctant to allow the “details” of risk allocation in connection with the negotiation of the contract “screw up their deal.” Such attitudes may cause the bank to back away, or readily compromise, on the issue of adequate remedies when “push back” is received from the service provider. It is useful for the bank and its attorneys, as part of their pre-negotiation discussions, to agree upon the bank’s “bottom line” in this area (as in other

areas of risk allocation) prior to commencing contract negotiations with the service provider.

LIMITATION OF LIABILITY AND EXCLUSION OF DAMAGES

Most service providers attempt to severely limit the recourse of the bank in the event the service provider fails to meet the SLAs. Although there are many variations, a not uncommon provision attempts to limit the institution's remedy to "service level credits," a refund of a pro rata portion of the monthly or quarterly fees paid by the institution for the period of the service failure, with a cap on the amount of total damages. If the service involves data processing and the failure involves the loss of the data or the incorrect processing of the data, the service provider may attempt to limit the bank to the exclusive remedy of the reconstruction or replacement of lost data, or the correction of incorrectly processed data. Some service providers may be willing to provide varying amounts of service credits, with the amount for each failure increasing, based upon the frequency or duration of service failures. Again, however, a cap on total damages is almost always included.

In addition to limiting its liability for breach of the SLAs, a service provider will customarily attempt to limit its liability for all breaches of its obligations under the agreement and for all claims "arising out of or related to" the agreement, which would include claims founded upon negligence or other tort liability. The provider's form of agreement often sets a "cap" on total damages (sometimes couched in terms of "liquidated damages") in the form of either a specific dollar amount (e.g., \$1 million) or a dollar amount equal to a set number of months of fees that a bank has paid (or would be expected to pay) to the service provider under the agreement. Some service providers will be willing to set the cap at an amount equal to all fees paid by the bank under the agreement. Where a number-of-months measure is used, it is not unusual to see caps in the range of nine to twelve months.

Suppliers invariably attempt to exclude liability for consequential, special or incidental damages (such as lost profits). Usually, the supplier is willing to extend the same exclusion to the banks; however, this is of less benefit to the service "receiver" than it is to the service "provider." On the other hand, the bank should insist that this exclusion should apply to both parties.

"CARVE OUTS"

As noted previously, the federal banking regulators expect that the bank's management will "assess whether the damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the service provider's failure to perform its obligations." This is not an assessment that is subject to mathematical certainty. Nevertheless, the bank's management should be prepared to answer an examiner's questions as to how it assessed the adequacy of the remedies provided in the contract in light of the limitations and exclusions that apply to the service provider's liability. As part of that process, the bank should demand that the limitations and

exclusions be subject to certain “carve outs” in those situations where the risk to the bank is potentially great and the justification for limitations and exclusions are less justifiable.

As to damages suffered by the bank, the bank has justifiable grounds for arguing that the exclusions and limitations that apply to the service provider’s liability should not apply to the following:

- Where the service provider is grossly negligent or engages in willful misconduct. Certainly, if the service provider agrees to be liable for its “negligence,” the bank should accept this provision. On the other hand, few service providers are willing to accept such liability. While some uncertainty exists (depending upon the state whose laws govern the interpretation and enforcement of the agreement) as to what differentiates “gross” from “ordinary” negligence, a good rule of thumb is for the bank to consider “gross” negligence as a willful or reckless disregard of its duty of ordinary care.
- Breaches of warranties and representations under the agreement. Such warranties will generally not relate to service levels, or, if they do, will be limited. Other warranties, such as the due authorization and enforceability of the agreement, the legal status of the service provider, the absence of conflicts with other agreements or laws, and similar matters, should not be subject to limitations or exclusions. Some providers will give a warranty that the services do not violate any third party’s intellectual property rights; however, the provider will attempt to limit the remedy for a breach of this warranty to the provision of a non-infringing modification of the service. Other providers will not give a warranty but will agree to indemnify the bank from third party claims based upon the alleged infringement of the services of the intellectual property rights of third parties. These rights are not equivalent and should be carefully considered.
- Breaches of the confidentiality and security provisions of the agreement. In light of the recent focus of state and federal regulators and legislators on the problems of privacy and security, especially with respect to customer information, and the potential exposure of the bank to monetary damages and damage to reputation, the service provider should be fully liable if it breaches its obligations in this regard. This assumes, of course, that the confidentiality and security provisions of the agreement are adequate.
- Death or bodily injury or physical damage to tangible personal property.
- Violations of laws. This provision can cause substantial negotiations over what laws are and are not covered, and the financial consequences of changes in the law. Sensitive areas, such as the Gramm-Leach-Bliley Act and the privacy and security requirements imposed by the regulators should be specifically addressed. Some vendors may attempt to limit their liability for banking laws of which they have not been informed by the bank, and to impose on the bank increased costs of providing the services that are caused by future changes in laws applicable to the bank. Banks often respond that a vendor in the business of providing technology services to banks should be, and stay, fully knowledgeable about such laws and should also bear the increased costs that are imposed by changes that apply to banks generally

(as opposed to a specific regulatory directives or orders that apply only to the particular bank).

- Indemnity obligations.

Some service providers will agree that their wrongful termination of services and failure to provide termination services also should be “carved out” of the exclusions and limitations on liability. Others consider “wrongful” conduct to be covered under the “gross negligence” exception. Others take the position that transition provisions are no different than any other provision of the agreement and should not be treated specially. The bank should evaluate the nature and importance of the third party services and the importance of the transition services (including, if appropriate, conversion to another service provider’s system) and insist on this carve out if it believes it is appropriate and necessary.

INDEMNIFICATION

In many agreements, the indemnification provisions cover the obligation of the service provider to indemnify the bank from its own losses and damages as well as from the claims of third parties. The bank has to be careful in such cases to understand what is and is not covered. As used by the federal banking regulators, the term “indemnification” concerns a contractual obligation of the service provider to defend and hold the bank harmless (including, from the costs and expenses of defending the bank) from claims by third parties that arise out of the negligence of the service provider. Most sophisticated service providers will not want the indemnification provisions to apply to claims for actual damages by the bank. As to third party claims against the bank, many services providers are willing to provide indemnification from third party claims that arise out of one or more of the following causes:

- Bodily injury or damage to tangible personal property caused by the negligence of the service provider, its contractors, subcontractors, agents or employees. Some service providers will provide indemnification against all claims but will only agree to extend the indemnity to those claims caused by its gross negligence. Inasmuch as this indemnity extends only to third party claims (and not to the banks own actual damages), the bank is justified in requesting that the indemnification extend to third party claims based upon the service provider’s ordinary negligence.
- Breach of the confidentiality and security obligations. Some service providers will attempt to limit their liability for the loss of data to the replacement or reconstruction of that data.
- Violations of law by the service provider.
- Alleged infringement or other violation of the service provider’s services (and/or software) of any patent, trademark, copyright, trade secret or other intellectual property rights.

The variations in indemnification provisions (and their relation to the representation and warranties provisions of the agreement) are many, and often are keyed to the “hot buttons” of the vendor’s risk management policies (or general counsel). Often, limitations are placed on specific indemnification obligations. In all cases, however, the bank should insist that

the indemnification obligations of the service provider are not subject to the exclusions and limitations of liability provisions of the agreement.

Therefore, while the “guidance” of the regulators indicates that bank examiners will expect to see the bank fully indemnified for the negligence of the vendor, such rarely will be the case. As is demonstrated from this brief discussion, while the issue is treated differently by individual service providers, few give a bank “full recourse” for breaches of the SLAs or other portions of the agreement or full indemnification for the negligent acts or omissions of the service provider.

SERVICE PROVIDER RESISTANCE

Some service providers have responded to banks that make reference to the guidance that it is merely guidance, not law, and, therefore, is not legally binding. While it may be technically correct to assert that such guidance does not, standing alone, have the force of law, it does embody principles established by the agencies as to what they consider to be practices that meet “safety and soundness” standards, which do have the force of law. The banking regulators have the ability to examine not only the institution, but also the service provider, and to take appropriate enforcement action against either or both for unsafe or unsound practices.⁴ Given the great deference that courts accord the determinations of the banking regulators in interpreting the laws that govern the institutions they regulate, it would be a foolish bank or service provider that did not take the guidance seriously.

This problem is not confined to banks and other financial institutions. *The Wall Street Journal* cited above observed that major technology customers were “fed up” with spending millions of dollars for software that contained flaws, and with the software vendors’ attempts to disclaim and/or severely limit their liability for such flaws. Chief Information, Technology and Security Officers at major companies such as General Motors, AT&T and Alcoa were demanding that “vendors should begin to stand behind their products as much as sellers of other products and services do.” The major corporations are frustrated with the technology service and product providers’ attempts to disclaim most liability for breaches of their service level agreements, for damages caused by their failure to perform, or for their own negligence. As noted in the article, although purchasers have some bargaining power when technology markets “soften,” the ultimate threat of “walking away” is difficult to carry out because of the cost of switching providers. In addition, some technology providers have a virtual monopoly in their areas, and can afford to dig in their heels. Banks are also facing these “facts of life.”

Exacerbating the perceived problem are recent data security breaches, which have increased in notoriety since the *Wall Street Journal* article was published. The banking regulators issued more “guidance”⁵ in April of this year that requires banks to implement response and customer notification programs to respond to unauthorized security breaches. Even experts within the technology industry agree that some liability may have to be imposed on the industry in order to get them to focus on security. “It’s still not top of mind,” said a Computer Associates International Inc. executive.

REGULATORY ASSISTANCE

If General Motors has trouble imposing an obligation of full recourse on its technology service providers, the problem for a community, and even mid-sized regional, bank is many times more difficult. It might be of assistance, especially to smaller institutions that lack bargaining power, if the banking regulators took notice of which vendors were and which were not willing to “step up to the plate” and provide their bank customers with adequate recourse in the event of failures to perform. Letting the banks, or the vendors themselves, understand that those vendors who are not willing to give banks adequate protection will not, over the long haul, be acceptable as service providers to banks, may cause a “paradigm shift” among vendors. Obviously, there is a limit to what the regulators are able to do, but the “little guys” could use some help in this area.

ENDNOTES

¹ FFIEC Booklet “Outsourcing Technology Services,” available at http://www.ffiec.gov/ffiecinfobase/html_pages/outsourc_book_frame.htm (last visited November 1, 2005).

² OCC Bulletin 2001-47, “Third-Party Relationships, November 1, 2001, available at <http://www.occ.treas.gov/ftp/bulletin/2001-47.txt> (last visited November 1, 2005).

³ David Bank, “Companies Seek to Hold Software Makers Liable for Flaws,” *The Wall Street Journal*, February 24, 2005, available at http://online.wsj.com/public/article/SB110920333716762568-4HmOtnPwm7wkRDGhzbipIC4s6I_20050326.html (last visited November 1, 2005).

⁴ See, for example, OTS Thrift Bulletin R-82a, “Third Party Arrangements,” September 1, 2004, where the Office of Thrift Supervision states that “[w]hen contracting for the services of a third party, be aware that OTS generally has authority to examine a third party’s activities, and where applicable, may pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by you or your third party.”

⁵ OCC Bulletin 2005-13, April 14, 2005, available at <http://www.occ.treas.gov/ftp/bulletin/2005-13.txt> (last visited November 1, 2005).