BRYAN CAVE

Reviewing Third Party Vendor Service Contracts

TABLE OF CONTENTS

Introduction 1
Contractual Requirements 1
Typical Elements of the Third Party Vendor Contract 2
Parties to the Contract 2
Vendor and Vendor Affiliates 2
Bank 2
Assignments 2
Recitals 2
Nature and Scope of the Work to be Done 3
Ancillary Services 4
Location of Where the Work is to be Performed 4
Domestic Locations 4
Subcontractors - Generally 4
Offshore Outsourcing 4
Dual Employees 5
Services Level 5
Vendor Reports 6
Breach and Termination 6
Non-Material Defaults 6
Automatic Termination Events 6
Termination for Convenience 6
Termination Assistance 7
Dispute Resolution 7
Foreign Based Vendors. 7
Choice of Law 7
Jurisdiction or Forum 7
Vendor Notice Requirements 8
Business Events - Strategic Changes 8
Business Events - Corporate Changes 8
Business Events - Adverse Changes to Business Operations 8
Business Continuity 8
Information Breaches and Compliance Lapses 9
Bank Notice Requirements 9
Audit Rights 9
Compliance with Laws and Regulations 10
Compensation 10
Ownership of Trademarks, Copyrights, Patents and Other Trade Secrets, Source Code Escrow Agreements 10
Confidentiality 11
Indemnification 12
Indemnification Limitations 13
Insurance 13
Customer Complaints 14
Bank Regulatory Oversight. 14
Zombies 14
Checklist for Vendor Service Contracts A-1

REVIEWING THIRD PARTY VENDOR SERVICE CONTRACTS

Introduction

Managing third party vendor relationships has always been an important function in banks. More recently it has become a hot topic for state and federal financial bank regulators. The increasing complexity of what vendors are doing for banks and the related attention to cybersecurity threats all contribute to the greater scrutiny. The 2016 white paper by the OCC, "Supporting Responsible Innovation in the Federal Banking system: An OCC Perspective," is just one of several guidance documents issued by the federal financial regulators over the past five years that focus to a large extent on third parties providing services and technology to banks. Significantly, some examinations have resulted in the regulators imposing settlements and impose civil money penalties on vendors. Previous to the OCC white paper, the CFPB issued third party guidance in 2012, the FFIEC provided guidance on IT service vendors in 2012 and the OCC and the Federal Reserve issued complementary guidance in 2013 on third party relationships and managing outsourcing risks.

Contractual Requirements

The OCC guidance is generally looked at as the "gold standard" for evaluating issues that need to be addressed in a vendor agreement. That does not mean that every contract a bank signs needs to have every one of those issues addressed or that each one needs to be resolved in favor of the bank. Vendor contracts come in many different shapes and sizes and may affect everything from back office processing, internet delivery systems, use of the "cloud" to the people watering the plants at the branch. Vendors will vary from small local operations to multi-national companies. The bargaining power of a bank obviously varies depending on its size. A small community bank is not going to have the same leverage negotiating a vendor contract with a national vendor as a much larger institution. That lack of leverage, however, is somewhat mitigated by the fact that large vendors understand what the regulators are looking for because they hear it from many of their bank customers. That does not mean though that they will always offer it in the first draft of an agreement! Finally, you need to keep in mind that there may be several different ways of approaching a particular issue and drafting the contract language, all of which may be produce an acceptable outcome. As a result, a typical contract may touch on all of the points found in the OCC guidance but the individual contract provisions will fall along a broad spectrum.

The OCC guidance provides a good road map to what state and federal bank regulators (not just the OCC) look for when reviewing a bank's significant third party contracts. Contracts for significant third party contracts that fail to address the OCC highlighted issues may result in a bank being criticized in an examination report and could be a factor in a CAMELS downgrade of management. Management also needs to be aware that defects in major contracts will come up in due diligence performed in a merger transaction and can affect the viability of a proposed M&A deal. Thus, the "risks" that are being managed are broader than the business risk that occurs because of a non-performance by the vendor and is a good reason why senior management needs to pay close attention to the negotiation of significant vendor contracts.

Vendors should also be examining the guidance and modifying their contracts accordingly because banks are going to be raising the same issues over and over again. Vendor personnel who are on the front lines negotiating contracts need to be aware of the regulatory scrutiny and understand why requests for alterations to the contracts are being made by the bank.

Again, please keep in mind that simply because an issue is flagged for discussion does not mean that the final outcome is preordained. There can be multiple ways of addressing an issue depending on the relative negotiating strength of the parties and the services in question. As with any contract, compromises will be made on the final terms. The most important outcome for a bank is to be able to show the regulators that a conscious decision was made about which issues were important for the contract in question and how the contract reached its final form.

Typical Elements of the Third Party Vendor Contract

Parties to the Contract.

Vendor and Vendor Affiliates. Let's start with what is supposed to be one of the most elementary issues, who are the parties to the contract? Occasionally, a bank will negotiate a contract only to find that the contract is actually going to be signed in the name of a subsidiary or affiliate of the party they were negotiating with. The bank may still wish to proceed with signing the contract but it should do only after considering whether the subsidiary is capable of performing under the contract and can satisfy any claims for indemnification that might arise due to vendor mistakes. If the bank has any concerns in this regard they may want to consider obtaining a guaranty or other written commitment by the parent company to financially support the subsidiary.

When dealing with a large company that has several affiliates, the bank should make at least a cursory review of how the various parts fit together and whether there are any affiliations that might cause regulators some concern.

Bank. It sounds simple, but you will be surprised how many times a vendor contract (at least the first draft) uses an incorrect spelling or completely different name for the bank. You should make sure that the contract names the bank correctly, including on the front page, the signature page and throughout the document including the notices section. All addresses, email addresses and other contact information should be filled in and correct. It is not unusual to see a contract that has the correct name of the bank on the first page but uses the name of another institution in other places in the document. These types of "artifacts" from other agreements can pose problems for the parties down the road, particularly if they affect the notice provisions. You want to know exactly who to call when there is vendor error and likewise, when the vendor is providing notice of upcoming downtime for software updates you want that notice to get to the right people at the bank.

Assignments. Typically the bank will not want to allow the vendor to be able to assign the contract unless they first obtain the written consent of the bank. The vendor will typically push back on this and seek pre-approval for an assignment to an existing affiliate. The vendor may also seek certain approval rights should the bank seek to assign the contract. Both parties will generally want to allow assignments by operation of law such as those that occur as part of a merger. The bank may have some concerns on this particular point inasmuch as there may be other vendors that the bank does not wish to do business with. It is not an easy point to negotiate but the bank may want to consider requesting the right to terminate the contract in the event of a merger. A bank's success in getting that type of provision added to the contract will vary depending on the size of the vendor.

Recitals. Some contracts will contain several "WHEREAS" clauses at the inception of the document followed by a recitation of various facts about the parties and what they are trying to accomplish by entering into the contract. From a pure legal standpoint, "WHEREAS" clauses are not required but many parties like

to include them to properly set the stage for what is to come afterwards. If they are included, the bank needs to review them, particularly those that describe the parties and the services that the vendor will perform. The recitals provide for an introduction to the parties and provide a high level overview of their agreement. It is a bit like looking at a topographical map and following two streams as they wind their way through the mountains before finally coming together.

If there is a gap between the direction indicated in the recitals and the body of the agreement then there may be legitimate questions about what the true intent of the parties was when they entered into the contract. That becomes significant when a dispute later arises about the work actually being performed as well as the service level of the work. The gap can be created when the vendor uses a version of the contract that was heavily negotiated for a different party but forgets to revert back to its standard form contract when submitting it to the bank. Sometimes it is evidence of lack of sophistication by the vendor who may have simply downloaded the contract off of the internet and uses it without fully understanding the legal implications. Sometimes vendors will respond that they have used a particular form for years and never had a problem. That is confusing luck with carefully draftsmanship.

Nature and Scope of the Work to be Done. What exactly are the services to be performed? One would expect that the contract will specifically identify the frequency, content, and format of the service, product, or function provided. It is vitally important that the people at the bank, who have the substantive knowledge about the services in question, together with legal counsel, review the scope of services and understand how it relates to other contracts the bank has entered into or strategic initiatives the bank is looking at. A significant factor to keep in mind is whether any fee triggered by an early termination of the contract is of such a size that it becomes a material roadblock to doing a merger or acquisition. There have been instances involving smaller community banks where the termination fee was so large in comparison to the consideration being paid in a planned merger that the deal fell though. Thus, other corporate strategic matters may drive the bank to negotiate a shorter agreement than the vendor normally seeks or to seek out another vendor altogether.

It doesn't matter how many discussions you have had with the vendor about the scope of the work, if you can't tell from the contract itself, whether it is in a numbered paragraph or on an exhibit, exactly what the vendor is going to do, the contract is too vague and needs to be revised. This is not something to be shy about. We tell clients and younger lawyers who are drafting documents to imagine someone sitting in a windowless room reading the contract. If that person could not figure out exactly what work the vendor is doing from reading the contract and its exhibits, the contract is faulty. The trap many people fall into is that after having had numerous conversations back and forth, they mentally fill in the details when they come to a section in the contract that is vague and think they know what the "agreement" actually is, regardless of what is actually put on paper. What happens, of course, is that both the representatives of the bank and the vendor can have slightly different recollections about what had been discussed and those differences can pose real problems once issues begin to arise during the life of the contract.

The description of the nature and scope should be fairly specific. A lack of clarity here means that the vendor may not be held responsible if it fails to deliver the services the bank was expecting. The parties should be as comprehensive as they possibly can in describing the scope of the services. In some contracts the parties will utilize what is referred to as a "sweep clause" which provides that certain services that are incidental to providing the specified services are also impliedly covered by the contract. The sweeps clause ensures that all services not described in the Contract, but necessary to provide those that are services described in the Contract are included in the quoted price. Without the sweeps clause, the vendor is only obligated to perform those services that are specifically defined in the Contract.

Descriptions that seem to come from a marketing brochure or state that they will be agreed upon post-closing may be too vague as to be enforceable The Bank should not be afraid to push back and demand that the contract spell out in detail exactly what products or services the vendor is going to be providing.

Ancillary Services. Include in the contract, as applicable, ancillary services as software or other technology support and maintenance, employee training, and customer service. Address whether training be onsite or remote. If the bank's employees need to be trained onsite the contract should specify how much training is going to be required, i.e., is it something that is going to take an hour or do they need to set aside an entire day to complete. If the training will be on the premises of the bank you should consider security issues. For example, will the person doing the training need to access bank computers or networks? Will they be uploading any type of training software onto bank computers? The bank should have in place information security policies that the vendor must comply with. The fact that someone is doing training does not mean you should allow them unfettered access to computers and systems. For example, security protocols might include restricting vendor employees to computers that have no internet access, printers or devices for removable storage; limiting the use (or prohibiting altogether) mobile phones that have cameras.

Location of Where the Work is to be Performed.

Domestic Locations. Where is the vendor actually performing the work? Will they need physical access to the bank premises or equipment? Will they be on-site during or after business hours? The contract should reference security policies governing access to the bank's systems, data (including customer data), facilities, and equipment. The vendor should be obligated to comply with the security policies when accessing such resources. If the work is being done at the vendor's office, the bank will want approval rights any change in the location. Depending on the type of services being provided, the bank may also want the contractual right to go to the vendor's offices to view the vendor's internal security systems.

Subcontractors - Generally. An important question for the bank to ask is whether any of the work is being outsourced to a subcontractor. If the vendor is using subcontractors, the bank should consider whether it will want notice of and perhaps approval rights over who is being used. In addition, the contract should make it clear that the bank considers the vendor responsible for the performance of the contract regardless of whether it outsources a portion of the work. The contract should also make it clear that subcontractors are subject to the same confidentiality and security requirements as the primary vendor. Consideration should be given to adding a contractual provision which requires any subcontractors to verify in writing that they will comply with the privacy requirements.

The fact that a vendor performs all of the work in-house today is not a guaranty that they will always do so. You should expect that the ways in which vendors provide services will continue to change and you should not assume that a topic does not need to be addressed simply because the vendor does not engage in that practice today.

Assuming that the use of subcontractors is addressed in the contract the bank should consider what will occur if the vendor uses the subcontractor in a fashion that is not authorized under the contract. The conduct may be such that the bank will want to be able to declare the vendor in default under the contract.

Offshore Outsourcing. Will the vendor, or a subcontractor of the vendor, be performing any of the work overseas? This has become such a commonplace occurrence that a bank should never assume that all of the work or the support function for the products and services it is negotiating to purchase are all occurring within the United States. Depending on what the product or services being provided to the bank entail, this

may be a minor or very major issue. For example, if the vendor has access to personal identifying information on consumers, are you comfortable with that information being sent overseas? Even if the information does not involve consumer information, are you comfortable with the security procedures used in the foreign operation? The contract should also prohibit the outsourcing of work to subcontractors overseas unless the bank is first made aware of the practice and consents. When work is being offshored, it is common to attach an exhibit to the contract describing in detail the security procedures used in the offshore location including what type of background checks are conducted and other internal security processes. The bank needs to know where its information is being sent and will want approval rights if the location is being changed.

Dual Employees. Certain types of vendor arrangements will involve using "dual employees," i.e., existing employees of the bank who also become employees of the vendor. The contract should clearly articulate their responsibilities and reporting lines. Issues that should also be addressed include how such persons are being compensated. In certain instances, it may be that the bank is not allowed to compensate the employee for certain matters but the vendor can. The contract should make it very clear that the bank is not making any sort of prohibited payments.

Services Level. Services levels should be defined. For example, are the service to be made available 24/7 365 days a year or are they only needed during normal business hours. When the services involve some type of software or online technology, what is the minimum amount of "uptime" required? Depending on the services involved, uptime might be 99.9%, for example. Vendors will understandably push back on that figure and might suggest 98%. The right figure need not be either one of those numbers and is dependent on the type of service being provided and its criticality to the bank's delivery of services to its customers. To the extent there is planned downtime for things such as software updates it should occur during off peak time periods. Service level measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Certain products and services have standards that are common across the industry while others may need to be developed to fit the particular transaction. Service levels should be revisited from time to time during the term of the relationship to provide an opportunity for them to evolve along with the services being provided.

Banks should consider what type of reporting they want the vendor to provide considering performance against the service level targets and what type of remedies to which the Bank is entitled in the event vendor fails to measure or report on the service levels. Banks should also consider including requiring a root cause analysis for incidents and service level failures. In other words, it is not just sufficient to report a failure, what caused the failure and exactly what needs to be done to remedy it. It can be very frustrating when a vendor's performance affects customers and the bank is unable to explain to those customers how a problem is being fixed so that it will not reoccur.

One option to consider when addressing service levels is whether the service level requirement is an "all or nothing" target or whether it is merely one factor in determining whether the bank is entitled to credits against its normal monthly billing for the services. For example, if the service level on average for any given month is at 95%, perhaps the bank receives a credit against fees owed. If the service level falls below 95% then the contract may provide that such an event constitutes a material breach allowing the bank to terminate the contract.

Vendor Reports. The vendor should provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. Thought should be given to how long the vendor is required to maintain the records. That will play into audit requirements. The reports should include performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.

One element of reporting concerns how quickly the vendor determines that a problem has occurred. Depending on the services being provided, one may expect that the vendor will have in place automatic monitoring of services. The detection of a defect should then in turn trigger a report to the bank together with a proposed temporary fix/workaround and a resolution of such failure in accordance with agreed upon timeframes.

Breach and Termination.

Non-Material Defaults. What happens if the vendor is unable to meet its obligations under the contract? In some instances this may simply be a monetary issue and treated by an adjustment of fees. Certain non-material defaults may simply trigger a notice and a right to cure as well as a minor adjustment on fees. Failure to cure the defect or provide a temporary fix might elevate the matter to a more material breach.

Automatic Termination Events. In certain instances, however, a bank may wish to have the absolute right to terminate the contract with the vendor. For example, a bank should be able to terminate a contract in whole or in part if the vendor has breached the confidentiality or data privacy provisions, or if the service level failures are of a significant magnitude or because of the vendor's intentional refusal to perform the services. Likewise, (i) the vendor's failure to remediate significant deficiencies within a specified period of time after receipt of notice; (ii) or material weaknesses in the vendors Service Organization Controls Report ("SOC"); (iii) the vendor's bankruptcy, (iv) a change of control without the bank's consent; (v) extended force majeure events, and (v) bank regulatory directives to terminate, should give the bank the right to immediately terminate the contract without incurring substantial penalties. Consideration should be given to how much notice is necessary and the time frame to allow for the orderly movement of the services to another third party vendor. Upon termination the vendor should be obligated to return or destroy the bank's data and other resources.

Termination for Convenience. Another typical provision is "termination for convenience." This simply means that the bank has decided for various business reasons that it no longer wishes to be party to the contract with this particular vendor. The bank needs to be aware, however that a termination for convenience usually will trigger some type of payment obligation on the part of the bike to the vendor. In some instances the vendor may require a pro rata portion of the unpaid fees for the life of the contract in order to allow for the termination. These fees can be significant and banks should review the exact terms of such provision very carefully prior to signing the contract. As part of the services, the contract should define the vendor's obligations to facilitate the orderly, uninterrupted transfer and transition of the services back to Bank or to another service vendor, including the continued provision of the services for a reasonable period of time to allow the transition to occur. The obligation to provide this termination/expiration assistance should apply regardless of which party terminates the contract, unless the vendor is terminating due to Bank's payment default.

Termination Assistance. Depending on the type of contract involved, the bank may need substantial cooperation and assistance from the exiting vendor to move the work being provided to either a new vendor or into the back office of the bank itself. The contract should clearly assign all costs and obligations associated with transition and termination so that the parties understand this allocation at the inception of the relationship. Upon the termination the contract should provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary.

Dispute Resolution. It is not unusual for the bank and the vendor to get into disagreements about whether the vendor is performing under the contract. While a formal mediation or arbitration process is always something that is available, a more practical approach is to establish a more informal process where each side designates relationship managers who are required to meet within a specified time period, say seven days after the notice of the dispute, to try and reach an agreement about the nature of the deficiency and the corrective action to be taken. If they are unable to reach an agreement they then prepare a written reports to senior management and management attempts to resolve the matter. The typical provision includes a statement that the parties will seek to resolve the problem in good faith for a specified period of time. The dispute only goes to mediation, arbitration or litigation if all of the informal processes fail.

Foreign Based Vendors. It is important when negotiating a contract with a foreign vendor that the contract include choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. You should understand, however, that such contracts and covenants may be subject to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of choice-of-law covenants, requirements on banks, protection of privacy of customer information, and the types of information that the vendor or foreign governmental entities will provide upon request.

Choice of Law. If at all possible the bank is going to want the choice of law provision concerning what law applies to the interpretation and enforcement of the contract to specify the state in which the bank is located. Large national vendors will generally do the same and will seek to choose the state where they are located. Does it really make that much difference? In some instances it might. Some states recognize different legal causes of action against a party and thus legal exposure may differ depending on the jurisdiction whose laws are being applied. It may very well be that the commercial law in both states are similar enough that is does not really make a big deal but you should certainly be asking the question if the vendor has sufficient leverage to cause the choice of law to be another state than where the bank is located.

Some states, such as New York, have adopted laws that essentially encourage parties to a contract, even ones that have no physical ties to New York, to choose the law of that state for the interpretation of the contract. Whether a particular court will honor the choice of law provision can be complicated issue that revolves around public policy concerns and conflicts of law provisions.

Jurisdiction or Forum. Jurisdiction is sometimes confused with choice of law but it is a separate issue. Jurisdiction addresses the question of where a dispute will be heard. For example, a typical provision might say that a dispute will be heard in the state or federal courts located in a particular city or state. A bank will generally seek to litigate contract disputes in its home state for several reasons. The first is cost. The bank generally already has local counsel that it can reach out to handle litigation. If the matter is going to be litigated in another state by lawyers who do not have a current relationship with the bank then expectations are that the costs will be greater. Out of state litigation also increases travel expenses and introduce other

inefficiencies. Finally, parties can be worried about what is commonly referred to as "home cooking" where the perception is that a local judge and jury might be inclined to protect the local party.

Vendor Notice Requirements.

Business Events - Strategic Changes. There are several categories of events the bank will want to be notified about. The first involves things like significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved. In certain instances the bank may want the ability to terminate the contract if the vendor merges with another company or if there is a change in control. Similar to a loan transaction, the bank has "underwritten" the vendor. Bank officers have has met the vendor's senior management and are comfortable with the general direction of its business. A merger or change of control may change the strategic direction of the vendor and the bank wants to make sure it knows who it is doing business with.

Business Events - Corporate Changes. The contract should address notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology. Related provisions in the contract would be sections that without bank consent would prohibit the assignment of the contract; changes in the listed locations of where work is being performed and the use of subcontractors not previously approved by the bank.

Business Events - Adverse Changes to Business Operations. This category requires the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions. The bank should already have a contingency plan in the event the vendor goes out of business but a timely notification requirement helps to insures that the bank will have adequate time to put the contingency plan into motion.

Business Continuity. The contract should address the issue of what happens if the vendor's business is affected by natural disasters, human error, or intentional attacks. The contract should define the vendor's business continuity and disaster recovery capabilities and obligations to enable vendor to continue delivery of the services in the event of a disaster or other service interruption affecting a location from where the services are provided. Force majeure events should not excuse vendor from performing the business continuity/disaster recovery services. The contract should include the vendor's disaster recovery plan defining the processes followed by vendor during a disaster including backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans. A contract may include provisions—in the event of the third party's bankruptcy, business failure, or business interruption—that allow the bank to transfer the bank's accounts or activities to another third party without penalty. Ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements. Depending on the critical nature of the serve being provided, the bank may also want to consider stipulating whether and how often the bank and the vendor will jointly practice business resumption and disaster recovery plans.

Another important element of business continuity is who is going to be responsible for notifying bank clients of potential disruptions in the vendor's operations when the vendor is providing a bank client related service.

Information Breaches and Compliance Lapses. The compliance and information security requirements of the contract should include obligations to promptly notify the bank in the event vendor becomes aware of or reasonably suspects an information or data breach or compliance issue has occurred. This is not something that the bank wants to discover from reading the paper or even worse, from a bank customer who calls. A breach raises a whole host of other issues depending on the type of information that may have been impacted by the breach. There may be both federal and state law implications requiring notification to customers arising out of such a breach. The out-of-pocket costs of investigating and reporting a data breach can be substantial and the contract should be clear about any indemnification obligations of the vendor. The bank may want to consider what type of insurance the vendor should carry in order to satisfy the indemnification obligation.

Bank Notice Requirements. A typical provision might call for the bank to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party. This may be such an unlikely event that vendors will only raise it as an issue in certain unusual situations. If the provision does get included it should define exactly what the events might be that would trigger the notice requirement.

Audit Rights. As Ronald Reagan famously said, one should "trust but verify." Depending on the type of contract and the nature of the services being provided, the bank may want to have the right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews).

If an audit is required, the bank will want to consider whether to accept audits conducted by the vendor's internal or external auditors. Obviously, the level of oversight will depend on the type of services being provided, the scope of the contract, the size and sophistication of the vendor. The bank may wish to reserve the right to conduct its own audits of the vendor's activities or to engage an independent party to perform such audits. Audit reports should include a review of the vendor's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.

The contract should be clear about who will conduct any required audit, it should not be an item left up to the parties to decide on an informal basis post-closing. If the bank is reserving the right to audit the vendor, the contract should specify that vendor must permit audits by bank's auditors, designees, and any government regulator, including allowing access to facilities, personnel, and records. The bank should be permitted to perform financial, operational, and security audits to verify that the vendor is complying with the contract. The vendor should be required to develop a remediation plan and remediate issues uncovered during any audit.

If possible, the bank would prefer that the contract contain an affirmative statement that the vendor is obligated to cooperate with the party conducting the audit.

The vendor is going to have several concerns about an audit provision, the first being who is going to pay for it. A typical provision provides that the audit is to be performed at the bank's expense but a variation of that would be to shift the expense to the vendor if the audit reflects material violations. The vendor will also

have concerns over how often the bank can conduct an audit and on what type of notice. The right to conduct an annual audit coupled with the right to conduct one more often if something has occurred such as an information breach is one common approach. Finally, the vendor will want to know what type of notice will be given for an audit. The bank may prefer to leave it more vague but the vendor will generally want either a specific number of days notice or at a minimum, a "reasonable" time period.

Compliance with Laws and Regulations. The contract will generally require both parties to comply with specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations.. This can be a hotly contested provision. Parties on both sides of the contract will oftentimes seek to modify this provision to make it a bit more forgiving. Compliance with all laws is an aspirational target but the reality is that in our very complex society, anyone can find themselves having run afoul of some law or regulation. Thus, a vendor may seek to limit the applicability of this requirement to those laws and regulations that are directly applicable to it and its operations. Second, both parties may seek to limit the applicability to material compliance with those laws and regulations. To the extent the bank maintains policies and procedures outlining laws and regulations it is subject to and how it complies, depending on the type of services being provided, it will also want to require the vendor to comply with those policies. This item will also be addressed in the bank's ability to audit the vendor.

Compensation. Compensation for the services can be as simple as a monthly or annual fee or can involve a complicated calculation based upon various usage levels and vendor support. The contract should fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. There may be separate fees incurred for on-site training as opposed to online training.

The contract should address any expenses that will simply be passed along to the bank. The contract should identify the types of taxes that will be borne by bank and whether those taxes are included in the fees or charged on pass-through basis. The contract should also identify which party is responsible for any tariffs, duties, and import/export fees imposed on the services.

You should scrutinize the contact to see if there are any expenses for materials or services from other parties being incurred by the vendor that they are trying to pass along to the bank. If there are such expenses how does the bank know what to expect? Are there any caps on such expenses? Preferably, all such expenses are simply assumed by the vendor as overhead and not passed along to the bank.

Banks should also be on the lookout for fee structures that might have the unfortunate effect of incentivizing risky behavior on the part of the vendor.

Ownership of Trademarks, Copyrights, Patents and Other Trade Secrets, Source Code Escrow Agreements. Typically, each party should own its pre-existing materials and derivative works thereof and materials developed by the parties or their contractors individually and outside of the contract, and each party should provide the other with licenses to its materials necessary to receive or provide the services during the term. The contract should include intellectual property provisions that clearly define each party's intellectual property rights for their pre-existing materials and materials developed as part of the contract.

Does the vendor currently own or have the right to use all of the patents, trademarks, copyrights, etc., needed to provide the services under the contract or are they using intellectual property assets owned by the bank? If the contract involves the use of software purchased from a third party which needs to be customized, does the vendor or the bank have the legal rights to do that? The contract should address who will own any intellectual property created by the vendor as a direct result of the contract. Oftentimes, but not always, that will be the bank.

In contracts where the vendor is providing or using software in delivering the services, issues may arise over ownership and the right to use the software. Banks will generally want the vendor to represent that the vendor has full use of the software and that it is providing the bank with a non-exclusive right to use it. Usually the vendor will be required to indemnify the bank in the event a third party asserts a claim that the bank's use of the software was improper. If a successful claim of infringement is made, the bank may want to either obligate the vendor to obtain alternative software to be able to continue providing the services or be able to terminate the contract immediately. As a practical matter, if a successful infringement claim is made, the vendor may simply need to obtain a license from the other party in order to continue providing the software to the bank.

The contract should provide that the data of the bank remains the property of the bank and that the vendor is prohibited from using such data for any purposes other than providing the services under the contract.

If the bank purchases software, it should consider establishing escrow agreements to provide for the bank's access to "source code" and programs under certain conditions (e.g., insolvency of the vendor). "Source code" includes not only the human readable source code for the software in question but also any customizations and enhancements that were done for the bank. The typical escrow agreement would require the vendor to deposit new source code if a new, different, upgraded, or customized version of the software is delivered to the bank during the life of the contract. If any of the source code is encrypted the vendor must also provide the escrow agent with the decryption tools and decryption keys. This type of arrangement ensures that the bank will be able to continue using and/or benefitting from the software even if the vendor goes defunct.

Confidentiality. The bank will want the vendor to maintain the confidentiality of all information provided by the bank. This includes preventing the vendor or its subcontractors from using the information in a manner that is not anticipated by the contract. The contract should require that the vendor has, and at all times will maintain, an information security program that includes appropriate administrative, electronic, technical, physical and other security measures and safeguards reasonably designed, at a minimum, to: (a) ensure the security and confidentiality of all confidential information (specifically including any data on the bank's customers); (b) protect against any unauthorized access to or use of such confidential information; and (c) protect against any anticipated threats or hazards to the security or integrity of such confidential information. The vendor's security protocols are oftentimes attached as an exhibit to the contract.

One very important element of this provision is a notice requirement on the part of the vendor in the event of an information breach. Security breach should be defined to include unauthorized access, disclosure, or misuse of bank data or information that can be used to access bank data. Such a breach may trigger reporting obligations on the part of the bank. The contract should require the vendor to investigate, remediate, and mitigate the effects of the breach. The vendor should be required to develop a plan for implementing the remedial actions for bank approval.

It is important to note here that what we are talking about here is not necessarily an actual loss of bank client information, but rather a breach of the vendor's systems in general. The practical concern is that if the vendor suffers a breach of its systems, it may presage a later use by a hacker to use the vendor's connection to the bank to piggybacking its way into the bank's systems. There have been a number of highly publicized information breaches that were accomplished by using this approach and it continues to be of great concern to the banking regulators.

The vendor should be required to allow the bank and its agents, access to the vendor's premises to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity and confidentiality of bank information. The vendor will also need to acknowledge that it may need to provide access to the bank's state and federal bank regulators. The vendor should provide the bank with notice that the regulators have requested such access.

Indemnification. Indemnification provisions in a third party services contract can be hotly contested. There is no question that banks should include indemnification clauses that specify the extent to which the bank will be protected from claims arising out of the failure of the vendor to perform, including failure of the vendor to obtain any necessary intellectual property licenses. Not surprisingly, they can be one of the most difficult provisions to reach an agreement on.

In its simplest terms, indemnification constitutes an agreement to allocate certain risks of loss among the parties. It is analogous to a guaranty but just like a guaranty, the fact that you have one does not insure a party that they will in fact be protected from loss. An indemnification from a company that has little in the way of assets is no different than a guaranty from someone who has very little net worth. It may have some psychological value but may be worthless from a practical standpoint. Indemnification provisions can be drafted so tightly that they provide little protection and they can be made subject to limitations to the point that the protection offered is illusory.

If you look at a typical indemnification provision you will see, depending on the products or services being provided, some of the following items addressed:

- claims resulting from bodily injury, death, or damage to personal or real property caused by the vendor
- vendor's capacity as an employer of a person.
- intellectual property (patent, copyright, trade secret infringement or other intellectual property right claim) infringement claims
- vendor's violation of laws, rules, regulations, or orders applicable to it.
- claims resulting from the vendor's failure to comply with the bank's policies
- vendor's breach of bank third party contracts for software, business methods or services used by the vendor
- vendor fraud, criminal acts, or intentional misconduct
- claims for vendor tax obligations arising from the provision of the services under the contract
- claims by vendor subcontractor or vendors relating to the contract
- vendor's failure to obtain any necessary consents needed to perform under the contract

- claims resulting from vendor intentional refusal to perform any portion of the services
- claims resulting from vendor breach of the intellectual property, confidentiality, or data privacy provisions
- claims that would have been covered by insurance but for vendor's breach of its obligations to maintain insurance.

Obviously, the types of losses possible from the operation of heavy equipment will differ from a contract which provides financial software and the indemnification provision should be tailored to fit the situation. A vendor may push back quite strongly on claims for injury and death when the product being provided is merely computer software. A bank might reasonably conclude that the risk of physical injury is so small that the indemnification section need not cover such claims. The decision to include an indemnification agreement should be tied in with a determination by the bank about the vendor's actual ability to meet its obligations under the indemnification section. The vendor may be strong enough financially on its own but typically, the bank will also want the vendor to maintain certain insurance coverage to support the indemnification obligations. Obtaining an indemnification from a party that is clearly unable to perform does not add a lot of value.

Indemnification Limitations. When negotiating indemnification provisions you should be aware that those obligations are oftentimes affected by "limitation of liability" provisions found elsewhere in the contract. A typical provision might limit the vendor's liability to an amount which does not exceed the amount of fees it has been paid by the bank for a certain time period. Likewise, the provision may be set up so that one party absorbs the first amount of damages up to a specified dollar amount with the other party absorbing the damages above that amount. Another typical limitation is that the vendor will typically want to exclude any punitive damages or contract claims for lost profits.

The actual limitation agreed upon and ultimate allocation of losses will depend on the negotiating position of the parties. Whether you are a money center bank or a small community bank, however, you will want to know where you stand vis-à-vis the vendor in the event damages occur.

When considering the dollar amount limitations, the bank may want to consider carving out certain events due to the outsize exposure the bank might incur. These would include events such as damages arising from a party's failure to pay required taxes; failure to comply with applicable laws, rules, and regulations; breach of the data privacy obligations and payment for remediation actions; misappropriation and/or unauthorized use or disclosure of confidential information, intentional misconduct, criminal acts, or fraud and reaches of the intellectual property provisions.

Carefully scrutinize any provision in the contract that requires the bank to indemnify the vendor. While the bank will typically seek to minimize its indemnification obligations, there may be situations where the vendor is unwilling to move forward unless the bank provides a certain level of indemnification. If indemnification is going to be required the bank should examine its insurance to determine whether the indemnification claims would be covered by the bank's policy.

Insurance. The requirement that the vendor maintain insurance is related in some ways to the indemnification provision but is also independent of that provision. The bank may expect that, depending on the scope of any indemnification limitations, certain of the obligations arising under the indemnification section may need to be satisfied by access to an insurance policy. Outside of the indemnification obligation, the bank will want to know that the vendor will be able to satisfy claims brought against it for any one of a

multitude of claims and still remain in business. A contract will generally stipulate that the vendor is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.

Customer Complaints. Who is charged with responsibility for responding to customer complaints? Specify whether the bank or vendor is responsible for responding to customer complaints. If it is the vendor's responsibility, specify that the vendor will receive and respond timely to customer complaints and forwards a copy of each complaint and response to the bank. The vendor should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes. The contract should address the time frame within which the vendor should respond to customers as well as when it will notify the bank of the complaint. The vendor should also inform the bank of the resolution of the complaint within a specified time frame.

The vendor should be expected to document how each complaint is made, whether by letter, email or phone call. Copies of correspondence to and from the customer should be retained and provide to the bank. The bank needs to have sufficient information to be able to respond to bank regulatory agency requests about a particular complaint. A typical contract provision might require the vendor to provide the bank with a quarterly summary of all complaints in the form and manner determined by or acceptable to bank. The bank will also want to be able to access all pending complaints and responses.

Bank Regulatory Oversight. A best practice is to go ahead and incorporate a provision in the contract whereby the vendor acknowledges the federal banking agency regulatory oversight. Some vendors will be surprised to find out that their activities are subject to such oversight and will push back on any such provision. As a practical matter, it does not matter whether a provision is included in the contract, the federal regulators take the position that they have the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises. It is more of a "heads up" type of provision just to make sure that the vendor is not surprised if the FDIC or OCC reaches out to them.

Zombies. Somewhat surprisingly, Federal bank regulatory guidance does not suggest how vendor service agreements should deal with zombies. This was apparently an oversight on their part and we have been assured that the interagency taskforce comprised of members from the Federal Reserve, the OCC and the FDIC are under intense pressure to come out with guidance now that the CDC has beaten them to the punch [see: http://www.cdc.gov/phpr/zombies.htm "Avoidance, Termination and Disposal."] While there are some commentators who believe that the force majeure clause sufficiently covers service disruptions due to zombie attacks, others believe that you should be more proactive. For example, For example, Amazon Web Services provides that certain restrictions of the use of its services no longer apply "in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization." We will leave it to you to decide whether you want to deal with zombies under force majeure or a more custom drafted provision.

For more information about this topic please contact:

Jerry Blanchard
404-572-6804
jerry.blanchard@bryancave.com

Bryan Cave LLP is a global law firm with approximately 1,000 highly skilled lawyers in 27 offices in North America, Europe and Asia. The firm represents publicly held multinational corporations, large and mid-sized privately held companies, emerging companies, nonprofit and community organizations, government entities, and individuals. With a foundation based on enduring client relationships, deep and diverse legal experience, industry-shaping innovation and collaborative culture, Bryan Cave's transaction, litigation and regulatory practice serves clients in key business and financial markets.

Checklist for Vendor Service Contracts

Think of this Checklist as a map. As with any trip, there are usually several different ways of getting to where you want to go. The issues listed below are all ones that should be considered when negotiating significant vendor contracts but where you end up on each item will differ based upon the relative size and sophistication of both parties and the business needs of the bank. The final agreement may not favor the bank on every provision. Regulators do not expect that the bank will win on every negotiating point. But, just as with a road map, regulators want to know that the bank understands the various options it has in getting to the final destination and that it has weighed whatever business, legal and reputational risks that may flow out of the choices that have been made concerning the final agreement.

	Issues	Comments
1.	**Contract Structure**. Confirm that the names of the parties to the contract are correct, the contract and all exhibits are complete and that the fundamental requirements for entering into an enforceable agreement have all been satisfied.	☐ **Vendor Name** – Make sure that the name of the Vendor is who the Bank understands it should be. Vendors will sometimes attempt to put the contract into the name of an affiliate or subsidiary. Make sure that the Vendor's full legal name is complete. ☐ **Financial Institution Name** – Make sure that the Bank's full legal name is complete. Some Vendors may not understand the legal difference between a bank and its holding company and may try and use the bank holding company as the party instead of the bank. ☐ **Signatures**. Confirm that the parties signing the Contract have the actual authority to bind the respective entities and that the titles and names are accurate. ☐ **Authority**. Confirm that the individuals signing both for the Vendor and the Bank are authorized. Certain contracts may be of such a size and significance that a corporate resolution authorizing execution should be obtained. ☐ **Addresses**. Make sure that the mailing address, internet addresses, fax numbers and phone numbers are correct for the sending and receipt of notices. ☐ **Title of Contract**. If the contract has a specific "name" such as "this "Agreement," make sure that internal references within the contract are consistent and that defined terms are used in a consistent basis. ☐ **Definitions**. Vendors will oftentimes use acronyms to describe various products and services. Make sure all acronyms are defined in the contract, either where they are first used or in a separate definitions section. Defined terms should be reviewed carefully to insure that the given meaning is what the Bank expects it to be. ☐ **Exhibits**. Make sure that all exhibits and schedules are numbered properly and are physically attached.

	Issues	Comments
2.	**Recitals**. Does the contract contain recitals?	☐ **Consistency -** Recitals are not required in order to form a valid contract but if they are used they should accurately reflect the transaction. ☐ **Facts**. Recitals will oftentimes make statements of fact about the history of the transaction and the relationship of the parties. Makes sure that all such assertions are correct. ☐ **Contract Artifacts** - Review the recitals and the contract generally to insure that there are no misplaced references to other financial institutions left over from previous versions of the contract. This is more common when parties are using word processing templates where a Vendor simply pulls up the last contract they entered into and replaces the names.
3.	**Scope of the Services**. Ensure that the contract specifies the nature and scope of the arrangement. For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided.	☐ **Internal Review** – It is important that the appropriate people within the Bank are consulted and sign off on the terms of the Contract. For example, one does not want a line unit negotiating and signing a contract on its own if the Bank has an internal contracts administration unit that is supposed to handle that function. Likewise, Bank personnel need to know when to consult with counsel or other subject matter experts, and inside and outside legal counsel. Finally, the appropriate party within the Bank needs to review how the contract integrates with other contractual obligations of the Bank. ☐ **Description of the Services** -The parties should be as comprehensive as they possibly can in describing the scope of the services. In some contracts the parties will utilize what is referred to as a "sweep clause" which provides that certain services that are incidental to providing the specified services are also impliedly covered by the contract. The sweeps clause ensures that all services not described in the Contract, but necessary to provide those that are services described in the Contract are included in the quoted price. Without the sweeps clause, the Vendor is only obligated to perform those services that are specifically defined in the Contract. ☐ **Incorporation of Brochures** - References to proposals or other materials that read like marketing brochures are generally inadequate for a contractual description of the services. Brochures are drafted to market a product and the descriptions of the product and services may not always be technically correct. ☐ **Contingencies** – When the Bank signs the Contract they generally expect that the Vendor will be able to perform immediately. There may be situations where the Vendor needs to hire additional personnel or purchase new equipment. Incorporating contingencies like this in the Contract should be avoided where possible. ☐ **Agreements to Agree**. An agreement to agree to specific terms after signing the Contract can be problematic.
4.	**Ancillary Services**. Include in the contract, as applicable, such ancillary services as software or other technology support and maintenance, customer service.	☐ **Responsibilities Grid or Matrix** – You should be able to answer the question of precisely who is going to provide all of the services under the contract. This is often captured in the form of a responsibility assignment matrix such as a RACI matrix (R – who is responsible; A – who is accountable if things do not go as planned; C – who are the parties with the financial institution that need to be consulted and I – who needs to be kept informed about the progress?)

	Issues	Comments
5.	**Location of the Services**. Specify which activities the third party is to conduct, whether on or off the Bank's premises, and describe the terms governing the use of the Bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the Bank's or customers' information.	☐ **Service Locations** – The contract should list the locations from where the Vendor will be performing the services. Any change in the listed location should require the Bank's consent. ☐ **Bank Resources** – The contract should set forth on an exclusive basis the equipment, facilities, office space, and office services/technology that Bank is required to make available for the Vendor's use. ☐ **Security Policies** – The Bank should have Security Policies governing access to the Bank's systems, data (including customer data), facilities, and equipment. The Vendor should be obligated to comply with the Bank's Security Policies when accessing such resources.
6.	**Location of Work**	☐ **Domestic location.** Is it clear where the work will actually be performed? ☐ **Premises.** Does the Vendor need access to the premises of the financial institution? During normal working hours or in the evening? ☐ **Subcontractors- generally**. Does the contract address the Vendor's use of subcontractors? Preferably, the contract should restrict the Vendor's use of subcontractors to only those that have been approved by the financial institution for the approved function. Any change in the approved subcontractors should require the Bank's consent. ☐ **Offshore Outsourcing.** If the Vendor outsources work overseas will the financial institution have control over what information is sent overseas or not? Consider adding an exhibit to the contract spelling out the security procedures that will be followed by the offshore company.
7.	**Dual Employees**. When dual employees will be used, clearly articulate their responsibilities and reporting lines.	☐ **Responsibilities** – The contract should spell out in detail the responsibilities and reporting lines for dual employees. There will be certain areas of responsibility that Bank may not want to have oversight over due to possible regulatory compliance issues.

	Issues	Comments
8.	**Service Levels**. Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.	**Service Level Methodology** – Define the processes for measuring the Vendor's performance: ☐ Service levels should support the financial institution's business goals and compliance obligations. For example, performance measures should not be structured in such a manner as to incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. ☐ Service level definitions and targets can be measured a number of ways, including percentage of "down-time" or an error rate per thousand matters processed. It should be a measurement which is easily calculated. The contract should be specific about the processes and tools used to measure and collect data for the service level measurements. ☐ Consideration should be given to the fact that as the financial institution grows the service levels may need to change. ☐ Industry standards may provide a reference point but the financial institution may have peculiar needs which should be taken into account. ☐ Vendor's reporting obligations (i.e., a periodic report documenting the Vendor's performance against the service levels). ☐ Performance reports should not only address performance levels but also what steps the Vendor has taken to cure any reported defects. ☐ The contract should spell out remedies to which Bank is entitled in the event Vendor fails to measure or report on the service levels. ☐ Vendor's obligations to perform a root cause analysis for incidents and Service Level failures and to remediate those deficiencies that are uncovered by the root cause analysis.
9.	**Records**. Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow Bank management to monitor performance, service levels, and risks	☐ **Data Retention Requirements** – The contract should include an obligation for Vendor to record and retain records for the period required by law or by Bank's Policies, but no less than a defined period of time following the termination or expiration of the contract.
10.	**Reporting**. Stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports	☐ **Reporting** – The contract should define the reports that the Vendor is required to provide to the Bank, including the required contents of the reports, the frequency of the reports, the Bank resources that will receive the reports, and any other information that Bank requires from the reports in order to comply with its regulatory reporting requirements.

	Issues	Comments
11.	**Breach and termination.** Address the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship.	☐ **Pricing.** Failure to meet service level requirements can be met in a number of ways including rebates and pricing adjustments and if of a material enough level, the right to terminate the contract for cause. ☐ **Automatic Termination.** Certain events such as a breach of confidentiality provisions, bankruptcy and regulatory directives may trigger an automatic termination. ☐ **Termination for Convenience** – The contract should include the right for Bank to terminate the contract for convenience. In such event, it may be appropriate for Bank to pay a reasonable termination fee proportional to any unrecovered costs of the Vendor due to the Bank's early termination, but not lost profits. ☐ **Vendor Termination Rights** – If Vendor is performing services that are required for Bank's ability to operate, Vendor's termination rights should be limited to breaches of Bank's payment obligations. ☐ **Termination/Expiration Assistance** – As part of the services, the contract should define the Vendor's obligations to facilitate the orderly, uninterrupted transfer and transition of the services back to Bank or to another service Vendor, including the continued provision of the services for a reasonable period of time to allow the transition to occur. The obligation to provide this termination/expiration assistance should apply regardless of which party terminates the contract, unless the Vendor is terminating due to Bank's payment default.
12.	**Dispute Resolution**	☐ **Dispute Resolution Process.** A formal dispute resolution process can be helpful in preventing service issues and ambiguities from escalating to contract termination. A typical process requires each party to designate a relationship manager who must first meet to try and resolve disputes before a matter is moved to senior management. Resort to formal mediation or arbitration should only follow once the parties are unable to resolve the matter by themselves.
13.	**Choice of Law**.	☐ **Governing Law** – The contract should specify that it is governed by the law of a state in the U.S., preferably in the state where the Bank is located. Local vendors will generally agree to use the law of the state where the Bank is located but large national vendors will oftentimes pick the state where they are located. Choice of law should generally not be a deal killer but the Bank should understand what risks it may be running if another state's law controls.
14.	**Jurisdiction and Venue**	☐ **Jurisdiction for Resolving Disputes – US Based Entities.** The jurisdiction for resolving matters in court should if possible be the state where the Bank is located. Jurisdiction in another state will generally increase the costs of reaching a resolution.
15.	**Foreign Based Vendors**	☐ **Jurisdiction for Resolving Disputes – Foreign Entities**. Include in contracts with foreign-based third parties choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of choice-of-law covenants, requirements on banks, protection of privacy of customer information, and the types of information that the third party or foreign governmental entities will provide upon request. Therefore, seek legal advice to ensure the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such arrangement.

	Issues	Comments
16.	**Notice Requirements**. Address the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions. Address the Bank's materiality thresholds and procedures for notifying the Bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the Bank.	☐ **Notice** – The Vendor may want the Bank to set out strategic business or operational changes that would affect the Vendor's ability to provide the services and define any required notice and/or other requirements if such an event occurs. ☐ **Business Continuity** – The contract should include Vendor's business continuity obligations, which define Vendor's obligations and commitments in the event catastrophic events, disasters, and other service interruptions occur. Vendor's business continuity obligations should provide for the continued delivery of the services in the event of a disaster at a Vendor location and the processes, including notification, that Vendor will follow in the event a disaster or other service interruption occurs. ☐ **Information Breaches and Compliance Lapses** – The compliance and information security requirements of the contract should include obligations to promptly notify the Bank in the event Vendor becomes aware of or reasonably suspects an information or data breach or compliance issue has occurred. ☐ **Business Continuity** – The Vendor's business continuity plan should define when notification of a disaster or other service disruption is required and include the procedures Vendor will follow to notify Bank. ☐ **Data Privacy** – The contract should define when a security breach is deemed to occur and when Vendor is obligated to provide notification to Bank and perform remediation procedures. For example, has a "breach" occurred if a third party accesses encrypted Bank data? ☐ **Bank Policies** – All Bank have well defined Policies that document the manner in which Bank complies with the laws, regulations, and standards applicable to it including Policies related to materiality thresholds and notification procedures. Depending on the type of Contract being negotiated, the Bank may want to include the Policies as part of the Agreement, and the Vendor should be required to comply with any thresholds and/or processes defined in the Bank Policies.
17.	**Vendor Changes**. Address notification to the Bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology.	☐ **Assignment** – Vendor should not be permitted to assign the Agreement (including by merger) without Bank's prior consent. ☐ **Service Locations** – The contract should list the locations from where the Vendor will be performing the services. Any change in the listed location should require the Bank's consent. ☐ **Subcontractors** – The contract should restrict Vendor's use of subcontractors to only those that have been approved by Bank for the approved function. Any change in the approved subcontractors should require the Bank's consent. ☐ **Change Control** – The contract should have a defined change control process that requires Bank approval for changes to the services and contemplates how changes to Policies or other compliance issues will be implemented and who will bear the costs of such changes. For example, if a change in law or regulation requires that Vendor modify the services, does Bank bear the costs of such changes if Vendor has to implement the change for all of its customers to remain in compliance with such laws and/or regulations? ☐ **Notice** – The contract should also define any strategic business changes made by Vendor that could affect Bank, Bank use of the services, and/or Vendor's ability to provide the services and any notice and/or other requirement if such an event occurs.
18.	**Data Ownership**. Address the ability of the third party to resell, assign, or permit access to the Bank's data and systems to other entities.	☐ **Data Ownership** - The contract should provide that Bank's data remains the property of Bank and that Vendor is prohibited from using such data for any purposes other than providing the services under the contract.

	Issues	Comments
19.	**Compliance With Law**. Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations. Ensure that the contract requires the third party to maintain policies and procedures which address the Bank's right to conduct periodic reviews so as to verify the third party's compliance with the Bank's policies and expectations. Ensure that the contract states the Bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and requires remediation if issues arise.	☐ **Compliance with Laws Applicable to the Vendor** – Vendor and its subcontractors should be required to obtain all necessary regulatory approvals and comply with all laws, regulations, and orders applicable to Vendor generally and in its capacity as a Vendor of the services under the contract, including specific laws applicable to the services like GLBA, BSA/AML, OFAC, and Fair Lending and other consumer protection laws and regulations. ☐ **Compliance with Bank Policies** – Bank should have documented Policies that define the manner in which Bank complies with the laws, regulations, and standards applicable to it, including Policies related to Bank's compliance with GLBA, BSA/AML, OFAC, Fair Lending and other consumer protection laws and regulations. Vendor should be required to comply with the Bank's Policies as part of the contract.

	Issues	Comments
20.	**Contract Compensation and Fees**. Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Consider outlining cost and responsibility for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed, including limits on any cost increases.	☐ **Fees** – The contract should define all charging methodologies and charging units in detail. The fees for the services should be limited to the specific fees and charges set forth in the contract. ☐ **Pass-Through Expenses** – The contract should identify the pass-through/out-of-pocket expenses for which Bank is responsible. ☐ **Taxes, Tariffs and Duties** – The contract should identify the types of taxes that will be borne by Bank and whether those taxes are included in the fees or charged on pass-through basis. The contract should also identify which party is responsible for any tariffs, duties, and import/export fees imposed on the services. ☐ **Implementation Fees** – Any implementation fees or incentives to implement the services in a timely manner should not cause cash flow or similar issues to the Vendor that would encourage Vendor to take undue risks for payment. ☐ **Fees** - The contract should specifically provide that the fees for the services are limited to the specific fees and charges set forth in the contract. Any fees or payments for audit and examination fees to be paid by Bank would need to be defined in the contract. ☐ **Financial Responsibility Matrix** – Define the parties' financial responsibility for procurement, maintenance, growth, refresh, operational expenses, and any other cost applicable to the resources needed to provide the services, including equipment, facilities, software, and personnel. This is often captured in a financial responsibility matrix defining each category of costs associated with each resources, which party is responsible for the costs, and how the costs are charged to the Bank. ☐ **Variable Fees** - The contract should specifically provide that the fees for the services are limited to the specific fees and charges set forth in the contract. Any volume based fees should be defined in the contract. ☐ **Services/New Services** – Only "new services" that are outside the defined scope of services that Bank has agreed to via an amendment should result in increases or additions to the fees that are outside the defined fees and charges. The contract should define a mechanism for the parties to resolve any disputes as to whether a service is in scope or out of scope that puts the parties on equal footing with respect to the dispute.
21.	**Ownership and Use of Trademarks, Copyrights, Patents**. State whether and how the third party has the right to use the Bank's information, technology, and intellectual property, such as the Bank's name, logo, trademark, and copyrighted material. Indicate whether any records generated by the third party become the Bank's property. Include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the Bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).	☐ **IP Rights in Bank Materials** – The contract should define the license rights that Vendor has in the Bank's materials. The license should limit Vendor's use of Bank's materials to use necessary to provide the services during the term of the contract. ☐ **General IP Rights**– Typically, each party should own its pre-existing materials and derivative works thereof and materials developed by the parties or their contractors individually and outside of the contract, and each party should provide the other with licenses to its materials necessary to receive or provide the services during the term. The contract should include intellectual property provisions that clearly define each party's intellectual property rights for their pre-existing materials and materials developed as part of the contract. ☐ **Escrow Agreements** - In certain software projects, the Bank may want to require that the Vendor place certain of the source code in escrow so that if the Vendor goes defunct the source code is released to the Bank.

	Issues	Comments
22.	**Confidentiality** Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines.	☐ **Confidentiality** – The contract should include appropriate confidentiality provisions that define Vendor's obligations to protect the Bank's information and prohibit unauthorized disclosures to third parties. Moreover, the contract should limit Vendor's use of Bank's confidential information to use for the purpose of meeting its obligations or exercising its rights under the contract. ☐ **Data Protection Requirements** – The contract should include obligations for Vendor to comply with applicable domestic and international laws and regulations pertaining to data privacy, personal data, transfer of information across international borders, data flow, and data protection and to implement practices and procedures sufficient to enable such compliance. ☐ **Information Security Management System** – Vendor should be required to maintain an information security management system that is consistent with industry practices and sufficient to comply with the data protection requirements of the contract.

	Issues	Comments
23.	**Information Breaches**. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. Stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party. Address the powers of each party to change security and risk management procedures and requirements, and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity.	☐ **Security Breaches** – The contract should require Vendor to promptly notify Bank if Vendor becomes aware (or reasonably suspects) that a security breach has occurred. Security breach should be defined to include unauthorized access, disclosure, or misuse of Bank data or information that can be used to access Bank data. ☐ **Remediation of Security Breaches** – The contract should require Vendor to investigate, remediate, and mitigate the effects of the breach. The Vendor should be required to develop a plan for implementing the remedial actions for Bank approval. ☐ **Updating Data Safeguards** – Vendor should be required to revise its information security management system and its data safeguards from time to time in accordance with industry practices and inform Bank of such revisions as part of the services, unless such a change would prevent the Vendor from meeting its obligations under the contract or compromise the confidentiality or security of Bank's information and data. ☐ **Incident Management**– The contract should define the joint obligations and responsibilities of the parties with respect to incidents involving intrusions or other security breaches. ☐ **Business Continuity/Disaster Recovery** – The contract should define the Vendor's business continuity and disaster recovery capabilities and obligations to enable Vendor to continue delivery of the Services in the event of a disaster or other service interruption affecting a location from where the services are provided. ☐ **Force Majeure Events** – Force majeure event should not excuse Vendor from performing the business continuity/disaster recovery services. ☐ **Disaster Recovery Plan** – The contract should include the Vendor's disaster recovery plan defining the processes followed by Vendor during a disaster including backup schedules and processes. ☐ **Termination/Expiration Assistance** – As part of the services, the contract should define the Vendor's obligations to facilitate the orderly, uninterrupted transfer and transition of the services back to Bank or to another service Vendor, including the continued provision of the services for a reasonable period of time to allow the transition to occur. The obligation to provide this termination/expiration assistance should apply regardless of which party terminates the contract, unless Vendor is terminating due to Bank's payment default. ☐ **Disaster Recovery Plan** - The contract should include the Vendor's disaster recovery plan defining the processes followed by Vendor during a disaster including backup schedules and processes. ☐ **Disaster Testing** – The contract should require that the disaster recovery procedures should be tested periodically and include obligations for Vendor to correct any failures identified during testing within a defined timeframe and re-test as necessary to ensure such failures have been corrected.

	Issues	Comments
24.	**Audit**. Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.	☐ **General Audit Requirements** – The contract should address Vendor's obligations to maintain an audit trail of all financial and non-financial activities resulting from the services. The contract should identify which party will perform the audits. If Bank can audit the Vendor, the contract should specify that Vendor must permit audits by Bank's auditors, designees, and any government regulator, including allowing access to facilities, personnel, and records. Bank should be permitted to perform financial, operational, and security audits to verify that Vendor is complying with the contract. Vendor should be required to develop a remediation plan and remediate issues uncovered during any audit. ☐ **Internal Controls Reporting** – The contract should define the types and frequency of internal control reporting (e.g., SOC 1, type 2, SOC 2, type 2, etc.). The reports should cover all Vendor locations from which Bank receives services. Vendor should be required to develop a remediation plan and remediate any qualifications identified in such reports according to such remediation plan and within a defined period of time. ☐ **PCI Reporting** – If the Vendor is storing or processing credit card data, the Vendor should be required to provide annual PCI Reports on Compliance and Attestation of Compliance for Onsite Assessments – Service Vendors. Any PCI compliance issues must be promptly corrected and remediated. ☐ **General Audit Requirements** – Define which party's auditors will be performing the audits and which party bears the costs of such audits. Are the audits included in the fees for the services? Define the types of audits that Vendor will perform or that Bank is entitled to perform. There should be no limitation on audits performed by or required by the Bank's regulators.

	Issues	Comments
25.	**Indemnification**. Consider including indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability. Examine limitation provisions.	**Vendor Indemnities** – The contract should include obligations for Vendor to defend, indemnify, and hold harmless the Bank, its affiliates, and its and their officers, directors, and employees from the following types of third party claims: ☐ IP infringement claims ☐ Claims by employees of Vendor related to the contract ☐ Claims resulting from bodily injury, death, or damage to personal or real property caused by Vendor ☐ Claims resulting from Vendor's violation of laws, rules, regulations, or orders applicable to Vendor ☐ Claims resulting from Vendor's failure to comply with the Bank's Policies ☐ Claims related to Vendor's breach of Bank's third party contracts for software or services used by Vendor ☐ Claims resulting from Vendor's fraud, criminal acts, or intentional misconduct ☐ Claims for Vendor's tax obligations arising from the provision of the services under the contract ☐ Claims by Vendor's subcontractor or vendors relating to the contract ☐ Claims resulting from Vendor's failure to obtain any necessary consents needed to perform under the contract ☐ Claims resulting from Vendor's intentional refusal to perform any portion of the services ☐ Claims resulting from Vendor's breach of the intellectual property, confidentiality, or data privacy provisions ☐ Claims that would have been covered by insurance but for Vendor's breach of its obligations to maintain insurance. **Bank Indemnities** – Depending on the nature of the services under the contract, it may be appropriate for Bank to indemnify Vendor for similar types of third party claims.
26.	**Indemnification Limits**. Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. Consider whether a contract would subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights.	**Limitation of Liability** – Depending on the nature of the services, a limitation on the amounts and types of damages may be appropriate. However, the Bank should consider whether damages arising from certain acts or omissions should be excluded from the limitations of liability. For example: ☐ Accrued charges and credits ☐ Indemnification obligations. ☐ Damages arising from a party's failure to pay required taxes ☐ Failure to comply with applicable laws, rules, and regulations. ☐ Failure to comply with Bank Policies ☐ Breach of the business continuity and disaster recovery obligations ☐ Breach of the data privacy obligations and payment for remediation actions ☐ Misappropriation and/or unauthorized use or disclosure of confidential information ☐ Intentional misconduct, criminal acts, or fraud ☐ Breaches of the intellectual property provisions ☐ Vendor's intentional refusal to perform

	Issues	Comments
27.	**Insurance**. Stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.	☐ **Insurance** – The contract should obligate Vendor to maintain appropriate insurance coverage for the benefit of Bank.
28.	**Default**. Ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination.	☐ **Warranties** – The contract should include warranties and covenants with respect to the performance of the service. ☐ **Operational Defaults and Service Level Termination Events** – The contract should include thresholds defined by objective performance measures (such as service levels) that indicate when a material breach has occurred or a series of breaches that in the aggregate have an adverse effect on the services that entitle Bank to terminate the agreement
29.	**Customer Complaints**. Specify whether the Bank or third party is responsible for responding to customer complaints. If it is the third party's responsibility, specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the Bank. The third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes.	☐ **Customer Complaints** – If Vendor is responsible for receiving and responding to customer complaints, the contract should require Vendor to maintain copies of the complaints and Vendor's response to the complaints and provide copies to Bank. In addition the processes and requirements for responding to complaints should be clearly defined as part of the contract. All information needed to analyze the reports that Vendor is required to collect and report to Bank should be clearly defined and captured in the contract.
30.	**Subcontractors**. Detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors Reserve the right to terminate the contract without penalty if the Vendor's subcontracting arrangements do not comply with the terms of the contract	☐ **Responsibility for Subcontracting** – The contract should specify that Vendor remains responsible for the acts and omissions of its subcontractors. Any rights and obligations of the Vendor should also apply to the subcontractors, which includes the Bank's right to audit subcontractors. ☐ **Termination**. The Bank may want the right to terminate the contract should if the Vendor's arrangement with subcontractors does not comply with the provisions of the contract. This presupposes that the contract is not silent about the use of subcontractors, whether domestic or offshore.

	Issues	Comments
31.	**Federal Banking Agency Oversight**. In contracts with Vendors, stipulate that the performance of activities by external parties for the Bank is subject to federal banking regulator examination oversight, including access to all work papers, drafts, and other materials. The federal banking regulators take the position that they have authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the Bank itself on its own premises.	☐ **Regulatory Oversight** – The audit provisions of the contract should include the right for applicable banking regulators to conduct examinations of the Vendor and any subcontractors, including access to the Vendor's and its subcontractors' facilities, personnel, records, and other materials.
32.	**Zombies.**	☐ There is a difference of opinion about whether you may want to deal with zombies under force majeure or a more custom drafted provision. Your choice.