BRYAN CAVE

BRYAN CAVE LLP One Atlantic Center, 14th Floor, 1201 W. Peachtree Street, N.W., Atlanta, GA 30309-3471
T: 404 572 6600 F: 404 572 6999 bryancave.com

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.

	Issues	Comments
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.
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.

	Issues	Comments
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.
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.

	Issues	Comments
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.
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.

	Issues	Comments
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
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

	Issues	Comments
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.
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.