NCONTRACTS

PROTECT YOUR INTERESTS:

How to Negotiate Cost-Saving Vendor Contracts

NCONTRACTS.COM
888.370.5552

EXECUTIVE SUMMARY

With the proper strategy, every financial institution can negotiate an advantageous vendor contract that protects from hidden costs, mitigates risks, and ensures that vendors are working to their full potential for the institution. This whitepaper explores the three key phases to contract negotiations: assessment, planning, and negotiation. It also reveals common vendor tricks and offers strategies for making the contract fairer.

INTRODUCTION

Whether your financial institution has one location or 1,000, your ability to maintain productive vendor relationships comes down to the quality of the vendor contract. It's about more than pricing. An effective vendor contract considers everything from your institution's strategic needs to regulatory requirements to liability issues.

The largest institutions have teams of lawyers and years of experience to identify and close loopholes that slant the contract in the favor of vendors – a luxury that smaller financial institutions don't have. These institutions are at a disadvantage when negotiating with vendors that close hundreds of deals a year. Vendors have developed standard contracts that lean strongly in their favor. They know what other institutions are paying, and they know just how to present a deal so that it looks attractive.

All is not lost, though. With the proper strategy, every financial institution can negotiate advantageous vendor contracts that protect from hidden costs, mitigates risk from the outset, and ensures that vendors are working to their full potential for you.

It comes down to three key steps:

1. **Assessment phase.** Before you talk dollars and cents with a vendor, you need to do your research. This whitepaper will show you how to assess the needs of your institution, assess the market players to find the most credible vendors, and think about how you'll measure return on investment (ROI). We'll also tell you how to define direct and indirect costs you may incur.
2. **Planning phase.** Once you know what you need and who you need to talk to, you need to research fair market value pricing and terms.
3. **Negotiation phase.** You've got a plan, now it's time to negotiate. We'll show you the most important factors when it comes to timing and negotiating pricing and terms. We'll also help you understand the true value (or nonvalue) of discounts.

THE ASSESSMENT PHASE

Assess Your Needs

Vendors are masters at luring you in with bells and whistles you don't really need. That's why you need to begin the process with an internal assessment of what your institution is trying to accomplish.

Begin with an exercise in defining your business needs by asking what elements you'd include if you were building the product or service yourself. Don't just say what you need. Justify why you need it and how it will help you define ROI. Make sure it's aligned with your goals. If you can't justify why you need it, it might not be a need.

Sometimes you might need to see what's out there to help you understand your needs. It's okay to see what's available, but tread carefully. You don't want to start chatting up vendors only to get distracted by a fancy user interface or other things you don't really need.

It's also essential to consider the risks of partnering with a third-party vendor. Data breaches, system failures or outages, regulatory compliance failures (ex: BSA/AML, consumer compliance, etc.) and vendors that outsource to other vendors are just some of possible risks – and your institution needs plans to mitigate them. Customers and regulatory agencies will blame the institution, not the vendor.

Assess what can be done to mitigate the risk and if the reward is worth it.

Assess the Market

There's no shortage of information about vendors. The key is narrowing down your short list.

Whittle down the list by seeking referrals and consider any vendor whose name keeps coming up. It's probably a leader in the market.

The best places to seek referrals are:

- **Other financial institutions.** Listservs, email groups, LinkedIn groups and networking events are great places to ask around.

- **Professionals associations.** Both state and national associations are familiar with vendors and can make referrals. Some conduct extensive due diligence, giving you added reason to check out a vendor.
- **Favorite vendors.** If you have a vendor you like, ask them who they recommend.

Once you have a list, don't just focus on what vendors have in common. Look for the unique characteristics that stand out to help determine who should be considered.

Define the Costs

Cost is a key component—though it's just one element. If you specifically negotiate pricing but not terms, you can still have a bad agreement. It will just be a little less expensive.

With that caveat, let's dig into the kinds of costs: direct and indirect. Direct costs are spelled out clearly in your contracts, while indirect costs are other expenses related to the relationship.

Here are some of the most common direct costs and the mistakes institutions make.

Recurring fees. All monthly, quarterly, annual costs.

One-time fees. These are often entry costs and include implementation fees, training fees, and data import fees. There are also unpredictable fees that are sometimes layered on top, often for items like compliance and audit reports. These all should be included in the contract.

Fee increases. Fees typically rise annually. Make sure the annual CPI increase costs or costs related to volume are reasonable.

Termination fees. Suppliers are notoriously vague on the cost of termination. Some say it's 80%, 90% or 100% of the remaining contract. But that doesn't include conversion, de-conversion or integration fees which are often set at the prevailing rate. Negotiate all these fees into your contract before you need them.

Indirect costs that affect the bottom line can include training, management oversight, and compliance. Think about how much time will go into these activities to assess the cost.

PLANNING PHASE

Benchmarking

Is a vendor giving your good pricing? You won't know if you don't shop or ask around.

It's not always easy to compare. An institution may get a great price on one platform, but additional modules might be way above market price. The key is to think about the overall cost, including all the potential add-ons.

NEGOTIATION PHASE

Timing

Timing is critical when it comes to vendor contracts. Vendors are trained to approach you when you are close to your expiration date because it leaves you with little time to change vendors. That's why you need to begin your assessment when there is still plenty of time left on your agreement. (In the case of a core processor, that's 24 to 30 months, and less for other providers.)

Why is this timing so important? It leaves you enough time to choose another vendor if you can't get the pricing or terms you need, your vendor is underperforming, or if you've switched strategic directions and are looking for a new partner or to end the activity altogether.

You do not want to automatically renew an agreement without at least a review, especially if it's for a core. You could be locked in for years and the costs could be very high. That's why it's essential to have programs in place to identify and track key contract dates (including expiration, autorenewal, and notice of termination dates) so you are never caught off guard and forced to continue a vendor relationship that doesn't fit or provide reasonable pricing.

Pricing

There are several strategies for getting the best pricing. One strategy is collecting pricing from

several vendors. That's helpful, but it's not always an apples-to-apples comparison. Different vendor offerings have different features. This is where your needs assessment comes in handy. It helps ensure you're evaluating software through the right lens, placing greatest value on the elements that are strategically valuable.

Leverage the competition. Don't threaten to leave a vendor unless you mean it, especially with your core vendor. Your core vendor is a critical partner and that's not how you want to manage that important relationship. However, explaining that you have data from other core vendors demonstrates that the incumbent vendor should not take your financial institution for granted. In fact, you should mention the competition. You should always disclose your potential vendors to give each party an opportunity to highlight what makes them stand out from the competition.

Seek out incentives. Depending on where you are in your contract life, your volume and what products and services you need, you might get great incentives. Use this to your advantage. Typically, longer terms agreements can lead to price concessions from a vendor.

Align interests. Do you have a different strategy now than you did when you signed your last contract? Make sure your vendor understands the change. For example, let them know that now you're concentrating on M&A instead of survival.

Understanding So-Called Discounts

Everybody loves discounts, but not all discounts are the same. When vendors offer a discount, look at them carefully to see if they are as valuable as they first appear. Common discounts include:

Flex Credits. Flex credits are great if they can be used in many different ways, but that's not always the case. Some vendors restrict their use. They might give you $100,000 in flex credits, but they can only be used against future purchases of products and services at retail (i.e. insanely marked up) prices. Those credits are only valuable if you have the foresight to know what you'll want to buy and pre-negotiate prices for these services. Otherwise, a flex credit is worthless.

Line item invoices. The best discounts are at the line item level. Just make sure discounts reward you for growth and don't penalize you. When you grow, you bring your vendor more business. You should benefit from economies of scale. Also, it is critical to negotiate how the bill will be presented to allow your financial institution to reconcile it back to the terms of the agreement and fee schedules. Some financial institutions will even ask for a sample billing statement as an agreed-upon schedule to the agreement.

Terms

As we mentioned, contracts are about more than the obvious dollars and cents. There are many other terms and provisions that can have a material impact on a financial institution. A successful agreement protects a financial institution while controlling costs. Let's take a look at eight key elements of vendor agreements:

Scope. Scope defines what a vendor provides with service, support, and software. It should be clear enough that a person, particularly a regulator, can understand the purpose of the agreement and what the vendor is delivering. Too often these agreements just say the institution is licensing software and obligated to pay. It should give the details of the service or software, including the benefits and support provided.

These details are key to ensuring that your vendor delivers on its value proposition and can help you hold your vendor accountable.

Performance and benchmarks. Financial institutions need a way to measure vendor performance. That's why a service level agreement (SLA) is critical. SLAs are documents that describe the level of service expected by a financial institution from a vendor, lay out the metrics for measuring that service, and list the remedies or penalties, if any, should the agreed-upon level of service not be achieved. These metrics can include uptime, response to requests, and volume – and they should be as specific as possible.

Most SLAs should really be called "service level objectives." They have goals that vendors aim for, but no real consequence if they fall short.

If your customers can't log into your mobile app or the institution fails to complete a transaction, the most the vendor will have to do is reperform the service. That's why contracts need to include economic consequences. Some contracts may offer termination, but that's a painful path and last resort.

A strong SLA has an economic credit attached to it. Consider the case of a bank that found itself in hot water with customers and regulators when its vendor sent out 20,000 statements to the wrong customers. It was a major Gramm-Leach-Bliley Act violation that took hours and hours to clean up. The vendor took responsibility for the mistake, paying out what was owed according to the SLA's terms: a paltry 19 cents per statement.

When negotiating for financial consequences, one way to make your point to the vendor is to state that you know the price for 99.9% uptime. Then ask what the price will be if it's up only 90% of the time. You want to know the discount if the vendor doesn't perform at the agreed level, and you want to get it in writing.

Confidentiality. Vendors try to limit confidentiality clauses to GLBA and customer privacy, but vendors have more than just your customer data. They also have private, proprietary information about your financial institution that you don't want to share publicly. Most contracts have provisions to protect the vendor's business strategy and trade secrets but nothing to protect your institution. Make sure your vendor follows the Golden Rule and extends the same courtesy to you. Keep it simple by having your counsel provide standard form language on privacy issues to insert in all your contracts.

Access to risk management data and reporting. How do you know if a vendor is living up to expectations or if there's a problem? A contract needs provisions for data access. It should cover both access to an institution's data (including how it's used and who has access to it) and data about the vendor, including compliance issues, major strategic or operational changes, and the types of reports your institution can expect from the vendor and how often. This makes it easier to monitor vendor performance.

Audit and remediation. Audit rights are essential in a contract with a critical vendor and those that pose significant risk. It's a good idea to ask for provisions requiring the vendor to share periodic, independent audits – specifying type and timeframes. It might also include the right for the institution to conduct its own audit.

Operational resilience and business continuity. A vendor might provide mountains of documentation on its business continuity plan (BCP) during discovery and due diligence, but if the requirement for a BCP isn't in your agreement, those efforts can stop at any time. That's why contracts should specify expected BCP protocols and standards including, recovery time objectives (RTOs), recovery point objectives (RPOs), how often the plan is tested by a third party, and how the vendor communicates its results to you. The level of detail should coincide with how critical the vendor is to your institution.

Indemnification and limits on liability. Indemnity is when one party takes the place of another party for the purposes of liability. When it comes to vendors, it's important to know if your institution will be liable for a vendor or if there will be times when a vendor will assume liability. There should be specific language for indemnification including notice provision and who controls the defense of the claim.

Consider the ATM patent suits where institutions with ATMs connected to the internet have been sued by firms demanding licensing fees because they own the patent for that technology. Institutions whose ATM vendors have no liability are left on their own to defend the claim. Other institutions have been sued for websites that aren't compliant with the Americans with Disabilities Act.

When selecting a vendor, it may be worth it to pay a little bit more to someone who will take legal and financial responsibility for their product or service. The bigger the vendor, the less likely they are to change the indemnification provisions in their standard contract. Those vendors may consider the liability of doing business with you larger than the value of the agreement.

Limits of liability refers to the maximum amount of damages that can occur in the result of a breach of contract. The amount should be reasonable based on the service being rendered, but that's rarely the

case in a standard contract. For instance, some vendor agreements limit damages to $1,000 on an outsourcing contract that's supposed to save the institution $300k. In that case, the economic impact of the exposure doesn't really justify the ROI.

Insurance. Vendors both large and small should have insurance to protect your institution. Not only does this provide a deep pocket if there's a problem, but it can also keep your vendor in business in the event of an error. They should have enough insurance, especially cyber liability insurance as part of errors and omission coverage, to cover a breach. They should also provide an annual certificate of insurance.

Sometimes you can tie limits of liability to insurance. A vendor might tell you it's liable for only 3 months of fees, but that it has an insurance policy with millions of liability coverage. In that case, you might be able to craft an agreement that ties them to the limits of their insurance.

Subcontracting. Unless it's specifically stated in the contract, vendors can transfer their rights and responsibilities to fourth-party vendors, including subcontractors and suppliers, and not even tell you. Imagine you have a three-year agreement with an extremely secure IT host. You even did an onsite visit. Eighteen months later they switch to Discount Server Warehouse which gets hacked 20 months into your contract. As a result, your customer data is shared all over the internet. You're facing regulatory liability and consumer lawsuits all because no one addressed the assignment clause.

Ideally your contract will include a notice of consent, requiring your consent and a period of time for due diligence. This is possible with smaller vendors but not with cores. At a minimum, fight for language guaranteeing that any new data center (or other vendor) will be at least as good as your old one to ensure quality standards. It helps if you can build a business case for your request, for instance a call center that will interact with customers as opposed to a back office that just deals with employees.

Legal compliance. A contract should clearly state that the vendor is obligated to comply with laws and regulations, provide notice of compliance issues, and require timely remediation.

Ownership and license. Who owns the data the vendor produces on behalf of the institution? Can the vendor use the institution's intellectual property or logo? The answer needs to be in the contract.

Dispute resolution. Specify how disputes will be resolved and the timeframe for resolution.

Customer complaints. Customer complaints need to be addressed quickly or it can damage your reputation or draw regulator or media scrutiny. Contracts should specify whether the vendor or institution are responsible for responding to complaints, the timeframe for response, and provisions ensuring the vendor notifies the institution when it receives a complaint related to the product and services it offers on the institution's behalf.

Foreign-based third parties. Contracts with foreign parties may be subject to the laws of the jurisdiction where the vendor is located. Make sure that's something your institution is equipped to handle.

Default and termination. A contract should outline how a relationship will end, including notification requirements, timeframes, costs, and return or destruction of data. It should also detail ground for default and remedies.

Contract Review

Identifying pricing and other provisions in a contract is a heavy lift. Contract review can take hours and hours, especially since vendor agreements can be hundreds of pages long and designed to be convoluted. Pricing is hidden throughout along with auto-renewals for a variety of products and services. Then there are all the provisions you need to make sure are in place and written to protect your institution.

Institutions have three choices when analyzing contracts:

1. Have a contracts lawyer read it
2. Read it themselves
3. Leverage software

The most cost-effective and efficient approach is using software. Lawyers are expensive and take

a long time to review documents. Even if your institution has a lawyer on staff, they aren't a contract expert and even if they were, they don't have time to read tens or hundreds of vendor agreements. Reading it yourself is not only time-consuming, it's dangerous if you don't have extensive contract experience. It's easy to miss key provisions or pricing.

That's why more and more financial institutions are turning to contract management software with contract analysis capabilities and trained by legal and contract management experts. Harnessing artificial intelligence, the software can quickly extract key information from third-party vendor contracts and agreements, making it possible for financial institutions to quickly and easily:

- Score contracts for risk and adherence to regulatory requirements
- Generate summaries of key contract terms
- Automatically create alerts for key dates
- Search contracts for key terms and provisions (including renewal dates and price increases)

The result is contract reviews in minutes instead of hours, with hundreds of pages condensed to just a few pages of the most important information. This reduces review time and allows non-critical contracts to be reviewed in-house while giving you the information you need to go back to a potential vendor and re-negotiate for better terms – whether it's getting rid of termination fees or guaranteeing that your vendor will maintain its business continuity plan. AI-based contract management makes it easy to identify contract weaknesses for negotiation and keep an eye on key deadlines to ensure autorenewals never sneak past without an opportunity to renegotiate pricing and terms.

CONCLUSION

Negotiating a fair and effective contract is entirely possible with the right strategies and tools. The key is understanding the strategic objectives behind outsourcing, conducting a needs assessment, identifying the potential risks, and then using that information to negotiate with a clear vision of the outcome.

You need to check your work before signing the contract, ensuring that the contract includes all the provisions that are important to your institution.

This is an essential part of vendor onboarding and just one element of the vendor management lifecycle (planning, due diligence, contract negotiation, ongoing monitoring, termination). Once a contract is in place, an institution needs to monitor the vendor, ensuring it's delivering on its promises, and keep an eye open for the next time the agreement must be negotiated or terminated.

Contracts are a strategic tool that significantly reduces the risks associated with outsourcing. By ensuring comprehensive, clear, and enforceable agreements, organizations can maintain control over outsourced operations, safeguard their interests, and foster successful, long-term vendor relationships while controlling costs.

ABOUT NCONTRACTS

Ncontracts provides comprehensive vendor, compliance, risk management, and lending compliance solutions to a rapidly expanding customer base of 4,000 financial services institutions in the United States. We help financial institutions achieve their compliance and risk management goals with a powerful combination of user-friendly, cloud-based software and expert services.

Our solution suite encompasses the complete lifecycle of risk, including vendor management, enterprise risk management, business continuity, compliance, audit and findings management, and cybersecurity.

The company was named to the Inc. 5000 fastest-growing private companies in America for the fifth consecutive year. For more information visit www.ncontracts.com or follow us on LinkedIn and Twitter.

ABOUT NVENDOR

Nvendor is a comprehensive SaaS-based solution designed to help financial services firms protect their companies, reputations, and clients by managing third-party vendor risk. Covering the entire third-party risk management (TPRM) lifecycle, Nvendor includes tools for vendor due diligence, risk assessment, monitoring, contract management, and reporting – ensuring that organizations can mitigate risk efficiently while maintaining compliance with relevant regulations and standards.