OSLER

Fintechs: Negotiating service contracts with financial institutions

MAY 12, 2022 9 MIN READ

Related Expertise

- Artificial Intelligence
- Banking and Financial Services
- Commercial Technology Transactions
- Financial Services Regulatory
- Fintech
- Technology

Authors: Simon Hodgett, Christine Jackson

"Fintech" refers to new technology aimed at improving the delivery of financial products or services, either by complementing or competing with those products or services provided by traditional financial institutions (FIs). This broad category results in a wide variety of business models and contracting approaches. Many fintechs contract with existing FIs and, in our experience, this type of contracting can result in mutually beneficial business relationships. It is also our experience that the negotiation phase of the relationships can present real challenges. The good news is that deal friction can be reduced by acknowledging the differing business models and concerns of fintechs and FIs, and by coming well prepared to engage with them.

Commercial contracts

FIs pursue agreements with fintechs for a number of reasons, including accessing novel technology capabilities with a nimble development team, collaborating on new product offerings, and accessing potential new, under-tapped customer demographics.

Because of the wide variety of potential commercial arrangements, there is no single type of agreement that is typical between fintechs and FIs. In our practice, we frequently see a wide variety of agreements, including outsourcing and complex services agreements, collaboration agreements, cloud services agreements, reseller agreements, marketing agreements and technology development and licensing agreements. There are common negotiation challenges and solutions, however, that are worth considering.

Understanding financial technology companies and financial institutions

Fintechs and FIs have differences in structure, history, philosophy, regulatory requirements and stakeholders.

Fintechs offering technology to FIs are usually not directly heavily regulated and must grow at a high velocity with limited resources. Revenue acquisition is essential for early stage fintechs, and budgets for complex and protracted legal negotiations are limited; speed to a deal is an important consideration. Solutions (including all important security-related functionality) may be works in progress. Decision-making is usually centered on a few individual stakeholders.

FIs, on the other hand, are heavily regulated; their regulators prescribe onerous requirements and standards that the FIs must meet, expect the FIs to comply, and have little tolerance for non-compliance. Service continuity, data access and security, regulatory

compliance, reputational risk and customer retention are always top of mind for FIs.

The regulatory environment is complex and constantly changing and includes some or all of:

- the *Bank Act* or other applicable statutory framework
- supervisory requirements, including from the Office of the Superintendent of Financial Institutions (OSFI) and the Financial Consumer Agency of Canada (FCAC)
- codes of conduct
- privacy legislation
- anti-money laundering legislation
- securities legislation
- investment dealer rules and regulations
- payment rules and regulations, and
- insurance legislation and guidance.

Regulatory compliance within the FI's environment requires a robust risk management framework, consisting of a complex and often decentralized array of policies, processes and approvals that must be followed when contracting with third party suppliers. Commercial service contracts typically require review from a wide range of key stakeholders, in addition to the deal team with whom the fintech is negotiating business terms (e.g., cybersecurity, audit and accounting, risk management, legal, etc.). Approvals for negotiation concessions and final execution can be rigorous and time-consuming.

These differences can be jarring for both fintechs and FIs when sitting down to negotiate and when faced with the often complex agreements that include complex and detailed regulatory and risk management requirements that the fintech must meet.

Material outsourcing and third party risk management

Currently with respect to the types of commercial arrangements considered here, OSFI is the principal federal government agency that regulates FIs. The OSFI guideline B-10 — Outsourcing of Business Activities, Functions and Processes — sets out broad guidance, expectations and best practices for FIs to manage risks related to material outsourcing. B-10 is fairly generally worded, so FIs typically have their own criteria and internal departments that assess whether a particular service arrangement constitutes a material outsourcing. Under B-10, it is critical that a fintech entering into an arrangement with an FI knows whether the FI is treating the arrangement as a material outsourcing, as this will import a number of onerous terms into the contract (e.g., subcontractor terms, audit terms, security terms, service location requirements, business continuity plans, etc.) and reduce the flexibility open to the FI with respect to negotiating or conceding on those terms. The determination of whether an arrangement is a material outsourcing, however, has never been entirely clear or consistent. OSFI B-10 applies to — but is not necessarily well suited for — cloud computing arrangements, with certain provisions requiring careful consideration for such hosted services.

On April 27, 2022, OSFI released a new Draft Guideline B-10 – Third Party Risk Management. Although currently in the consultation phase and so subject to change, the new Guideline B-10 expands coverage from material outsourcing to third-party arrangements generally. The proposed new B-10 includes increased emphasis on FI governance and due diligence for third party arrangements. The new B-10, among other things, emphasises risk assessments, due diligence, and consideration of concentration risk (i.e., potential over reliance on a supplier, geography or subcontractor). It also includes (in Annex 2) a list of minimum

provisions for third party agreements, although these clauses describe topics which should be covered rather than specific clauses. The full impact of the new B-10 will become more apparent as the consultation period is completed. What is clear is that the exercise of determining whether an arrangement is a material outsourcing no longer will be a distinguishing factor in determining how a third party arrangement is treated. This will broaden the types of fintech arrangements affected by OSFI requirements.

In addition to OSFI B-10 revision, OSFI has increasingly focused on cybersecurity risk, including the Technology and Cyber Security Incident Reporting Advisory, as well as circulating a proposed Guideline B-13: Technology and Cyber Risk Management. The advisory and proposed guideline directly impact service providers and FIs alike.

Before entering negotiations

Generally, fintechs must consider the regulatory environment of their business and design systems and policies from an early stage in their development. Fintechs planning on providing services to FIs must also consider the regulatory constraints likely to apply to the proposed arrangement with the FI and anticipate how these will be satisfied in the contracting process.

In conjunction with preliminary business discussions, a fintech should also ask the FI about its stakeholder review process (e.g., whose approval is required and how long the approval process is expected to take) at the outset of negotiations and raise any relevant key issues for clarification and expectation alignment. Key issues and points of alignment may include:

- the overall nature of the services
- the objective of the arrangement
- subcontracting considerations
- cloud computing and SaaS arrangements
- security terms
- data flows, ownership and use, and
- audit rights.

Fintechs should consult advisors in advance to get a sense of what contracting terms can be anticipated from the FI, given the context of the services, the types of cybersecurity requirements that will be expected, and whether the arrangement is likely to be viewed as material outsourcing or otherwise high risk.

Form of service contract

FIs often wish to work from their own form of template agreements that are typically comprehensive, lengthy and designed to address stakeholders' interpretation of regulatory requirements. These forms of agreements are not always right-sized to the deal, which can result in protracted negotiations. Early on in the discussions, it is important to determine whether the use of such an agreement is understandable and reasonable under the circumstances or whether a more streamlined agreement could be used. To satisfy the need for quick assessment of a fintech's offering, it is worth considering whether a pilot program agreement or other short-form agreement might achieve the immediate goals of both developing the fintech's solution and affording the FI an opportunity to assess the value of the service in its business more fully.

During negotiations

During negotiations, fintechs should seek to understand where the FI has limited flexibility (e.g., regulatory requirements and the comprehensive nature of security requirements). Fintechs should focus their time and energy on addressing potential dealbreakers and items of business importance, rather than negotiating areas where FIs will not have flexibility.

Audit and security terms

Consider the FI's security requirements and aim to have all necessary security and plans for audit (e.g., SOC audits, if appropriate) in place prior to commencing negotiations. At a minimum, fintechs should be prepared to tell their security story and explain how it will mitigate risks, even if its arrangements are not in full alignment with the FI's requirements. Typically, a fintech that has a sophisticated security team can come to terms on details that fulfill the intent of the FI's security requirements, if not initially the same in every detail. Speak to counsel about potential alternative arrangements that FIs may be able to live with and that work with the fintech's technical abilities and resources. If the fintech is unable to absorb the high cost of implementing the FI's critical audit and security requirements until it has a guaranteed revenue stream, the fintech should consider proposing a staggered audit and security implementation plan.

Data

Data use and ownership raises complex issues for both FIs and fintechs, and there is no one-size-fits-all solution. Both parties should be prepared to spend a significant portion of the negotiations on this topic, and the fintech should be able to explain the value that the FI will receive in exchange for sharing its valuable data (e.g., lower costs or improved services). As part of the initial business discussion, fintechs should have a general conversation about value and the ways that it will be permitted to use the data, other than for the purpose of providing the services set out in the contract. Fintechs should be prepared to answer the FI's questions about data location, data use and data flows, as well as data security; if possible, create a data flow diagram that can be proactively provided to the FI to address these inevitable questions.

Consider the aspects of data use and ownership that will be important to the fintech during the course of the service arrangement, and whether it would be appropriate to have the FI provide a licence to use the data rather than ownership rights over the data. In most cases, licensing is an appropriate approach, as fintechs generally do not need to own the data to achieve their objectives, and the parties have the ability to draft the licence rights broadly or narrowly based on their preferences and needs.

Fintechs should also consider the regulatory frameworks that may apply to certain types of data, and that will impose obligations on the fintech or the FI (e.g., required safeguards for and restrictions on the collection, use, disclosure or transfer of personal information of customers or employees; financial and trading data reporting requirements; and other requirements related to data loss detection and prevention and cyber incidents). It is critical for a fintech to design its policies and services with data management best practices in mind; for example, only collect and use the data that is needed and for which it has all required consents, use aggregation and anonymization, limit data retention, and have data destruction and disposal plans in place.

Trends

FIs are continuing to show interest in acquiring technology innovations, and the sector has gained experience and comfort in this space. FI teams are now more familiar with the risks and rewards of undertaking service arrangements with fintechs and are showing greater flexibility and openness to deviating from traditional arrangements by using short-form agreements, pilot programs and sandboxes. Many FIs now have special affiliates or divisions dedicated to agile technology projects and are coming to terms with cloud computing. Meanwhile, the open-banking movement, greater adoption of artificial intelligence and payment reform are all on the horizon. By understanding the interests of their two (often vastly) differing businesses, cultures and requirements, fintechs and FIs can conduct smoother negotiations and achieve mutually beneficial business collaborations.