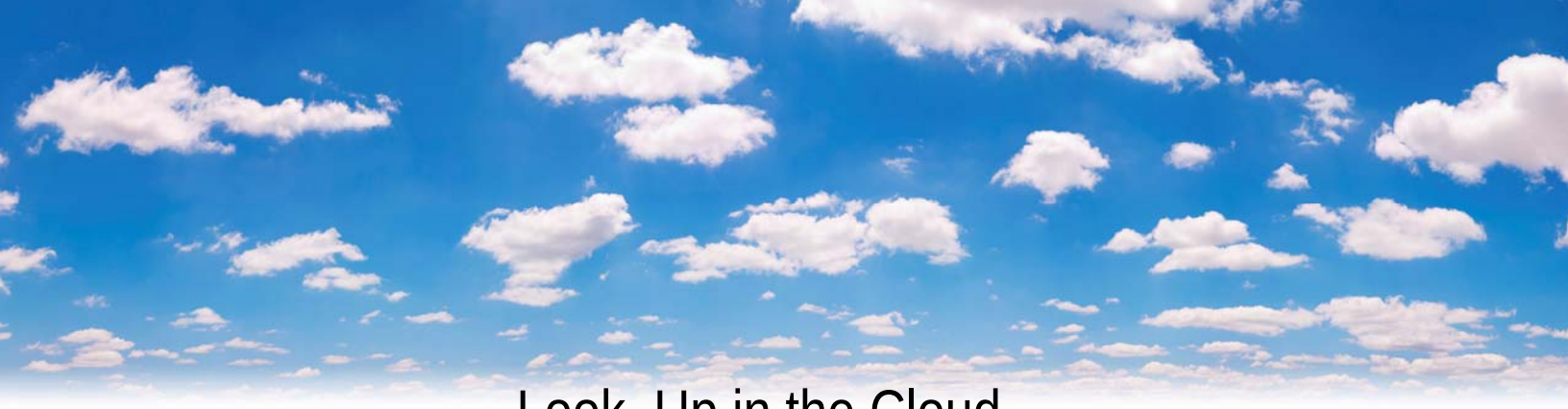
Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

Look, Up in the Cloud...
It's a Bird, It's a Plane,
It's a Bank

ReedSmith

reedsmith.com



Look, Up in the Cloud… It's a Bird, It's a Plane, It's a Bank

Chapter Authors

Joseph I. Rosenbaum, Partner – jrosenbaum@reedsmith.com

Leonard A. Bernstein, Partner – lbernstein@reedsmith.com

Anthony Traymore[1]

Introduction

The financial services industry, being one of the largest global consumers of technology, often serves as a driver of change as new banking and financial products and services are introduced into the information, transaction processing, storage and communications pipeline. Cloud computing as both a product and service of sorts will likely be no exception. The value propositions presented by utilization of cloud computing environments, such as cost containment, immediacy, availability, scalability, efficiency and resiliency, will simply be too attractive for chief operating and information technology officers to ignore. However, as highly regulated businesses, financial services firms will be forced to develop sound policy and governance practices to manage the risks that come with utilization of a third-party IT platform.

The Cloud Computing Primer

There are essentially four models of cloud computing environments available to financial services firms—private, community, public and hybrid.[2] The defining characteristic of a private cloud is that it is operated solely for one organization.[3] A community cloud is often shared by several organizations and supports a community with shared requirements.[4] A public cloud is made available to the general public or a large industry group.[5] A hybrid is some combination of two or more of the three other cloud environments—private, community and public.[6] Private clouds, because they are developed and used solely for the benefit of one organization, extend the most security of the cloud environments. As the sole user of a private cloud, an organization can often set the parameters for information collection, storage, transfer and access to suit its own policies and procedures. Also, the information stored on a private cloud will only be that of the single organization. Community clouds, to the extent the organizations utilizing the community cloud are able to agree, may offer similar data-protection parameters to that of a private cloud. However, a community cloud contains the information of all participating organizations—which means that a firm's information will be stored with that of other organizations, potentially even competitors' at times, if the community cloud is set up to handle the requirements of a specific industry. Public clouds generally offer less flexibility and robustness with respect to customization of information security processes and procedures, but understandably offer greater affordability. They are also more typically limited to the standard options offered by the third-party service provider.

Applicable Legislation and Federal Agencies

When considering cloud computing, the litany of primary legal risks that businesses in the financial services industry, along with their finance, business development and IT professionals and, of course, their lawyers, focus on, cross the spectrum from integrity and reliability to security, identity and privacy (*i.e.*, the handling of non-public personal information ("NPPI")). In the United States, financial services firms are subject to extensive laws, regulations and guidance relating to information security. The Gramm-Leach-Bliley Act of 1999[7] (GLBA) requires that financial institutions safeguard the security and confidentiality of customer information and places certain

prohibitions on sharing NPPI with non-affiliated third parties. Moreover, various state privacy laws, such as the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth,[8] also apply to the extent they impose more stringent security standards than GLBA. To the extent an institution—in some cases these same institutions—conducts broker-dealer activities; underwrites or offers insurance; engages in corporate and consumer banking; lends money; engages in the transmission of money; provides financial advisory, investment or custodial services; issues credit, charge, debit, stored value or gift cards—these and other laws, regulations and requirements apply. Businesses engaged in providing financial services in the United States are subject to these and an increasingly complex web of regulations and guidelines issued by numerous governmental and regulatory bodies, both individually and collectively,[9] such as the Federal Reserve Board, OTS, OCC, FTC, SEC, FFIEC,[10] FDIC and even self-regulatory initiatives developed and implemented by the Payment Card Industry (PCI).[11]

The challenge of compliance and corresponding risk necessarily becomes greater when a firm moves certain operations and functions to third-party cloud computing service providers. Each of the aforementioned statutes and regulatory bodies, as well as the numerous other regulations and guidance documents—several of which are referenced in this document—make it clear that an organization must conduct extensive due diligence on its IT service providers and use at least reasonable efforts to manage and monitor its third-party services providers' compliance with applicable guidelines and regulations. As far as the regulators are concerned, it will ultimately be the financial services firm's responsibility to handle NPPI of its clients and customers in accordance with applicable guidelines and regulations, regardless of whether such information resides on an in-house system or a third-party service provider system. As we said above, we don't know of any cloud-computing exceptions or carve-outs that would conveniently *manage* the many laws and regulations that govern financial services companies.

The principle of "follow the money" has become not only more facile in our age of digital processing and technology, but also increasingly complex. Both Congress and the online gambling industry discovered this back in 2006 when lawmakers finally realized, after years of failed efforts to stymie this explosive business, that the key to encumbering its growth was to stop the processing of financial transactions. The solution—tack an Unlawful Internet Gambling Enforcement Act onto the Security and Accountability For Every Port Act of 2006,12 which President Bush signed into law October 13, 2006.

Of potentially greater long-term consequence, the financial crisis, coupled with the perceived failure of the current regulatory scheme, helped garner support for the creation of the Consumer Financial Protection Bureau ("CFPB"). Created as part of the Dodd-Frank Act passed by Congress in 2010, the CFPB, housed within the Treasury Department, may well prove to be the most powerful federal agency in the United States. The CFPB has a single mission—to protect consumers. The scope of the CFPB mandate includes the development of consumer protection rules currently the domain of seven different federal agencies. With little oversight, a very large budget, and almost complete independence, the CFPB is likely to have a major impact on the financial services industry—from the manner in which financial services are advertised and marketed, to the disclosures and consumer protection mandates; from the nature of financial services and product offerings to compliance and enforcement measures. That said, it is also important to note that the CFPB doesn't actually replace any of the other agencies—it is intended to be incremental or supplemental to them, adding potentially another layer of regulation, compliance and confusing turf wars to an already complex financial services regulatory landscape.

The Landscape – Reconciling Regulations, Business Requirements and the Realities of the Cloud

Computing Globally

What, then, are the implications for cloud computing? Cloudy, to say the least. With cloud computing platforms, financial institutions may have the capability not only to outsource their technology operations and resources to the cloud, but also to significantly enhance their ability to reach consumers and offer financial products and services anywhere, anytime, with significantly pared down physical infrastructure. Web-based and mobile banking are already rapidly increasing in both availability and consumer adoption. The issue becomes of paramount importance as there is no exception or special dispensation for financial services companies that wish to adopt and integrate cloud computing into their infrastructure. Security, coupled with interoperability, will be as heightened a concern within the cloud as in any other environment, and very possibly more concerning.

Consider the following example: a financial institution wants to outsource its technology and operations to an

outsourcing provider in India. In evaluating the transaction, the financial institution needs to evaluate not merely the capabilities of the outsourcing provider to ensure integrity, security, transmission capability and reliability, but both the ability of the provider to ensure compliance with the banking or financial regulations that apply, and the question of whether the laws and regulations, the judicial system, and law enforcement mechanisms from the jurisdiction in which the outsourced services will be provided, are adequate to ensure that if the contract is solid, the ability to actually enforce it will be as well.

But what if the jurisdiction(s) is a continually floating cloud. As configured today, it will be difficult, if not impossible, to determine or regulate features, functions, services, applications, databases and the like, in a cloud computing environment. Will regulators need to insert a compliance regulator in every cloud-computing company? Will requirements and reporting be so complex and multi-jurisdictional that the perceived benefits of cloud computing will quickly be eaten up by difficult and overwhelming regulatory requirements, perhaps differing ones for differing jurisdictions? Do we need some international convention that countries and states will ratify to normalize cloud computing on a global (or quasi-global) basis? Will governments require cloud computing providers to agree to submit to jurisdiction before a regulator will allow a financial institution to use that provider's services? Will interoperability and cross-service platform agreements need to deal with these issues when one cloud computing provider interfaces with another?

Perhaps we can borrower a paradigm from the telephony universe where point-to-point communications often pass through multiple jurisdictions, carried by multiple carriers, transparent to both the initiator and recipient of the phone call. We rely on the privacy of these communications, in part because of technology, but also based on the fact that most voice telecommunications services are both regulated and protected around the world – most, but not all. Thus, if your telephone call was to be routed through a country that did not have such protections or had different protections – wiretaps, illegal in this country, might not be illegal and could even be routine practice for a foreign intelligence service, a private telecommunications company, or three teenagers with a homemade scanning device! This, in an industry that has been heavily regulated for almost a century. In stark contrast, cloud computing is not a regulated industry or activity. Which brings us nicely to consideration, briefly, of international issues applicable to cloud computing in the financial services industry.

As noted above, financial services firms with operations outside the United States must also be concerned with the foreign laws and regulations governing their operations in every jurisdiction in which they do business - in some cases, not merely different, but inconsistent laws and regulations. For example, the restrictions on firms with operations in Europe with respect to data transfer/sharing and security under the various country-level implementations of the EU Data Protection Directive, are more stringent than those under U.S. law. Suffice it to say, compliance with all applicable information security regulations and guidance, whether federal, state or abroad, is difficult for a financial services firm even in a self-contained IT environment; and yet a firm's failure to properly manage this landscape can be devastating.

Something Old, Something New – How Are Dated Rules and Regulations Applied to Cloud Computing

Returning the focus back to the United States, issues that financial services firms will be forced to grapple with are outdated and less-than-helpful regulations and laws. By way of example, the Federal Financial Institutions Examination Counsel ("FFIEC") over the past decade promulgated a series of guidance statements and policies for financial services companies on IT risk management for outsourced technology services, the latest of which was seemingly released back in 2004 (before the term cloud computing was even a glimmer in anyone's lexicon). While many concerns remain as genuine and applicable today as they did in 2004, there are just as many that get lost in the…clouds. The FFIEC, for example, calls for "clearly written contracts that provide sufficiently detailed assurances for performance, reliability, security, confidentiality and reporting."[13] In contrast, most cloud computing agreements (and perhaps private cloud agreements to a lesser extent) are take-it-or-leave-it documents that heavily favor the provider with robust disclaimers of warranties and limitations of liability. Other federal statutes, like FINRA's Notice on Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers, issued in 2005, requires NASD members to design supervisory systems and due diligence plans that include monitoring a service provider's compliance with the terms of any agreement…and assessing such provider's fitness and ability to perform the covered activities being outsourced.[14] Even the largest and most capitalized financial services firms will think twice about cloud computing if they are required by statute, rule or guidance to audit and monitor hundreds of data centers around the world for the *cost savings* it anticipates enjoying back at home. We did say cloudy, right?

The Necessity of Teamwork – Working with Your IT Professionals To Determine the Optimal Cloud Framework

When making determinations regarding the type of cloud environment to utilize and adopt (private, public, community or hybrid), and the applications and/or business functions that are suitable to be hosted in a cloud environment, it is essential that the financial services firm and individual lines of business look to its information security officer or director and his/her operational, compliance and legal teams for participation and guidance. When selecting a vendor, a financial services firm needs to be reasonably certain that the selected vendor has the capabilities to ensure compliance with all applicable laws and regulations that govern the firm's operations. Because cloud computing is a rapidly growing IT services sector, there is a large (and ever-expanding) pool of service providers from which to choose—including major players such as Oracle, Google and Amazon, and existing end-to-end IT infrastructure service providers that are eagerly pushing into this sector with the hope of capturing market share. While it might be tempting to leverage an existing relationship with an IT services vendor that may not have a long track-record with respect to cloud computing, the firm should be wary that it does not become a test case for such a service provider and, essentially, end up funding cloud-computing R&D. It also should be noted that, even more so than with respect to other, more established, IT services, standard terms and conditions in cloud-computing service agreements provide little in the way of customer protections and remedies. Therefore, it is critical to have strong negotiators and legal representation on these deals to ensure that the firm gets what it needs with respect to service levels, warranties, remedies, and other terms and conditions.

A Financial Institution's Preliminary Cloud-Computing Check List

Once the cloud computing project team is formed, the financial services firm needs to develop its requirements, specifications and due diligence checklist to measure the various third-party service providers. While these documents will be specific to the organizational standards, line-of-business requirements, and the specific business functions that it seeks to move into a cloud environment, the following suggestions may be helpful:

- Determine which business functions might be suitable for different cloud environments and classify your information assets by sensitivity. *For example, processes that require high-capacity processing but are utilized only periodically may benefit greatly from a cloud environment where capacity is available on-demand. On the other hand, functions that involve the collection and treatment of large amounts of NPPI may require use of a private cloud, or may not be suitable for transfer to a cloud environment at all.*

- Establish a robust and comprehensive set of requirements specific to the lines of business and specific business functions the firm would optimally operate, either partially or wholly, in a cloud environment. *It may be beneficial to develop the service level agreement in advance so that all the operational and regulatory requirements are on the table once you begin your vendor selection process. With this approach, it will quickly become apparent which vendors clearly are not able to satisfy your requirements.*

- Develop detailed and extensive governance processes and procedures, including meaningful goal-setting, policy and standard development, audit rights, frequent steering committee meetings, and clear escalation procedures.[15] *Considering the relatively nascent state of evolution of cloud computing services, it may be even more critical than with other more developed IT services, to drive the service requirements. Do not let a vendor get away with the "that's not market" approach.*

- Establish some form or protocol that allows the financial services firm to identify where its infrastructure and data are situated, both technologically and operationally. *You cannot simply launch and run your business purely on faith*.

- Consider not only the service provider's capabilities regarding robustness of information security, but also how readily your firm's information is able to be retrieved in the event of an investigation or natural disaster. *If your firm is subject to a regulatory investigation, the service provider must be able to cooperate and facilitate the investigation by providing the information required by the regulatory agency without compromising other information.*

- Adjust or develop your firm's internal policies to address the unique issues posed by the purchase and utilization of cloud computing services. *Because business owners may now, potentially, bypass IT entirely and purchase pre-packaged cloud services to perform certain tasks, the parameters around this process need to be clear.*

Conclusion

Adoption of cloud computing within the financial services industry is still in its infancy, as evidenced by a survey, carried out earlier in 2010, of several IT professionals within financial services firm. The survey, which sought to uncover the top information technology and security priorities for today's financial services companies, found that essential IT functions, such as security and compliance, continue to be the top concern for IT departments industry-wide. The survey reported:

- 34 percent of respondents believe that cloud computing is not strategic to their company, while 26 percent of respondents believe their company is risk-averse to cloud computing
- 58 percent of respondents only plan to invest in essential IT functions, such as security and compliance
- More than 75 percent of respondents are concerned about increasing government regulation

While at first glance these statistics provide somewhat of a dark outlook for the future of cloud computing within the financial services industry, it cannot be stressed enough that these numbers likely reflect the loggerhead of this new technological paradigm pitted against an increasingly complex, confusing and perhaps ill-equipped regulatory framework within which to operate. The fact remains, however, that the financial services industry continues to be very competitive and increasingly geographically independent. More than ever, financial institutions need to be agile as they expand both their girth and their global footprint. At the same time, internal IT projects are taking longer as IT resources get stretched to the limit. In many cases, cloud computing and SaaS-based deployment models have the inherent potential to give institutions the agility they need, while freeing IT from the somewhat mundane tasks of managing infrastructure and allowing them to focus on the strategic needs of the business unit. That, however, must be coupled with the extensive and steadfast due diligence and ongoing monitoring of a cloud provider's services to ensure continued compliance with the applicable laws and regulations governing a firm's operations. When asked to explain the survey results, LogLogic[16] CEO Guy Churchward aptly summarized them as follows: "While the cloud holds many benefits for the enterprise, we're not surprised to see that financial services firms are hesitant to adopt cloud computing. There are still many lingering questions about data security and transparency in the cloud, and it's up to cloud providers to offer visibility into these practices before we see mainstream adoption from financial services firms."

Only time will tell how widely adopted cloud computing becomes within the financial services industry, but as the offering continues to mature and improve, it's likely to be too enticing a service to be left unconsumed by financial institutions large and small.

— Biography of Authors —

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

Leonard A. Bernstein, Partner – Philadelphia +1 215 851 8143 · lbernstein@reedsmith.com

Len is a member of the Financial Industry Group and a member of Financial Services Regulatory Group. Len founded and chairs the firm's Financial Services Regulatory Group and concentrates his practice in the representation of banks, thrifts, mortgage bankers and finance companies in providing consumer credit compliance advice on federal, Pennsylvania and New Jersey laws and regulations. The FSR Group addresses credit card, auto finance, deposit, residential mortgage and other retail finance products. Len is nationally known for expertise with federal Truth-in-Lending Act, Real Estate Settlement Procedures Act and similar laws, and works regularly with federal and state financial services regulators.

— Cloud Computing Task Force Leader —

Joseph I. Rosenbaum
Partner and Chair, Advertising Technology & Media Law Group
jrosenbaum@reedsmith.com
+1 212 702 1303

— Endnotes —

[1] The authors wish to acknowledge the efforts of Anthony Traymore in researching and helping to prepare this article. Anthony, a former associate of Reed Smith, now serves as in-house counsel at Sony Corporation.

[2] ISACA, Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives (2009).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] 15 U.S.C. § 6801-6809.

[8] 201 CME 17.00 (2009). The Massachusetts law requires, inter alia, encryption of NPPI, up-to-date firewall and malware solutions, and for a business to take reasonable steps to ensure that third-party service providers comply with the requirements.

[9] *See*, *e.g.*, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule, 12 C.F.R. Part 30, et al. Requirements include exercising due diligence with service providers, requiring service providers by contract to implement appropriate measures, and monitoring service provider compliance. Appendix D, Section III (D).

[10] *See*, *e.g.*, FFIEC *Information Technology Examination Handbook* (2003–2010).

[11] *See*, The Payment Card Industry Data Security Standard, Version 1.2.1 (August 2009). Requirements include encryption of credit card account data when transmitted, and restriction of access to cardholder data to personnel on a "need-to-know" basis.

[12] SAFE Port Act, Pub.L. 109-347.

[13] FFIEC Guidance on Risk Management of Outsourced Technology Services, FIL 81-2000, 11/28/2000.

[14] No. 05-48, 7/05.

[15] *Id.*

[16] LogLogic, Inc. is a technology and application development company located in San Jose, California, that offers a comprehensive suite of log and security management products.