Cloud Computing – Transcending the Cloud:  
A Legal Guide to the Risks and Rewards of Cloud Computing, Part One

By Adam W. Snukal, Joseph I. Rosenbaum and Leonard A. Bernstein

Adam W. Snukal is a senior associate, based in New York, within the global Advertising Technology & Media Group at Reed Smith. Adam’s legal background includes diverse, complex and extensive experience in both business law counseling and in advising on advertising, technology and media-related matters. Adam’s experience in the area of information technology spans both strategic and commercial software licensing, large-scale procurement, e-commerce-related matters, financial services, health care and medical devices, wireless technology, outsourcing and gaming. In the area of advertising, Adam regularly counsels clients on traditional, online and mobile marketing/advertising-related matters, advertising and marketing agreements, media buying, trademark/brand licensing, user-generated content, privacy, sweepstakes, contests, gaming and advergaming, website and WAP site development, digital content development/distribution/aggregation, celebrity endorsements and more.

Joseph I. Rosenbaum chairs 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, including advertising, entertainment and media, financial services, travel-related services and technology. 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, he has authored a book on outsourcing (Outsourcing Agreements Line by Line (Aspirotre Publishing, 2004)), and a law journal article on privacy (Privacy on the Internet: Whose Information Is It Anyway?, Jurimetrics Law Journal, 1998). Joe is regularly quoted in publications such as the National Law Journal, Advertising Age, the American Banker, and Euromoney and has appeared on CNBCs 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 is a member of Reed Smith’s Financial Industry Group and a member of Financial Services Regulatory Group. Len founded and chairs the firm’s Financial Services Regulatory (FSR) 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 his expertise with the federal Truth in Lending Act, the Real Estate Settlement Procedures Act and similar laws, and works regularly with federal and state financial services regulators. He is a member of the Governing Committee of the Conference on Consumer Finance Law.

I. Introduction — Cloud Computing

Unless you have been living in a fog, you probably have not escaped hearing
about Cloud Computing. At the risk of spoiling the punch line, Reed Smith created its Cloud Computing initiative, based on observations and a growing belief that Cloud Computing is and will continue to fundamentally alter the business, economics and operations of companies around the world. Cloud Computing is not a technological phenomenon any more than Social Media is a technical innovation. Cloud Computing, like Social Media, is driven and enabled by technology, but represents a fundamentally significant shift in the manner in which technology will be used by nearly everyone in the years and decades ahead. The result will be shifting and unique legal and regulatory challenges, affecting fundamentally different business, economic and operational relationships, e.g.: between providers and business enterprises; between business enterprises and their customers; between their suppliers and business enterprises and customers; and even internally within each business enterprise itself. In this and subsequent articles, we aim to dig well below the surface of many of the legal, regulatory and contractual implications presented by Cloud Computing.

So what is meant by “Cloud Computing?” One of the simplest definitions comes from a 2010 Yankee Group report, that defines “cloud computing” as “dynamically scalable virtualized information services delivered on demand over the Internet.” Unless one is extraordinarily conversant with the technology, that definition may leave you a bit numb. So a few analogies may be helpful. You buy a toaster and plug it into the wall socket. The utility company hasn’t a clue you bought it, nor do they know if it’s a small one or a commercial grade toaster. You didn’t use it today, but tomorrow you will. You also have an air conditioner that’s on a thermostat—it cycles on and off depending on the temperature. You might live in a single-family home or an apartment house with more than 100 units. The electricity demands may vary greatly by unit or even by individual, and within a few miles or a few thousand miles; the ebb and flow of the demand for electricity is locally unpredictable and dynamically variable. But through years of capacity planning and statistical modeling, with interlocking and interconnected networks among the various utility companies, electricity is there, with rare exception, when and where you need it. Seamlessly, dynamically responding with as much or as little as needed, on demand.

You buy a sophisticated set top/game console for your entertainment center. You can watch television programming, rent movies on demand, play games locally or even across the Internet. It doesn’t hold any content. The content arrives, on demand, through signals sent to an array of virtual servers and processors, from a diverse set of program platforms, publishers and providers. In fact, you are so tech savvy, you even have a locally secure and encrypted Wi-Fi network in your home so you can stream the music, video, gaming and programming content anywhere you put a device capable of receiving the signal, and displaying or playing the content in response to the command of your remote control.

You have no idea where the player that displays Gone With The Wind is located, nor do you know where the servers are that connect you, in say, Minnesota, to gamers in, say, Argentina, France, Thailand and Australia. You can watch broadcast network television, cable, or satellite, or stream music from a variety of sources and access the Internet, right from your living room—or any room. You don’t worry about who owns the content or how it happens that when you want content, you can access it with the press of a button or the click of a mouse. Virtual, on-demand service: what, how, when, and wherever you want it. But you do pay a subscription fee, a license fee, or an on-demand fee, or some combination of these, to obtain and use the content.

Now add to these analogies the notion that large-scale digital storage has become increasingly inexpensive. The speed, capacity and ubiquitous availability of high-speed Internet access is already commonplace in many countries and developing in others, while processors connected to the Internet independent of time zones or geography can move and process digital bits of information and programming at speeds and in a manner inconceivable less than a decade ago.

Today, your information and data (your content) can reside in a cloud, i.e., in virtual storage independent of any particular server and potentially across many. The applications you need, whether you need them daily or once every month, and whether very simple or extraordinarily complex, will likely reside in such a cloud too. You can access them, share them, communicate with others, use, process and manipulate, collaborate, edit and display material anywhere—just plug in, enter your unique user identification (ID) and password combination, and it is there, at the press of a button and the click of a mouse.

Add to this the growing functionality of mobile and wireless devices, and one begins to get a glimpse of the future of cloud computing. You will no longer be tethered either to location or cumbersome devices. Indeed, you can use yours or anyone else’s portable input/output device—think Smartphone, netbook, touchpad and more. The programs you need, the data you have created or stored, the communications capability you need are all there in the cloud. Devices will not require increasing processing or battery draining capability, it’s all in the cloud. Indeed, most “apps” represent links to data or services, or both, that are accessed but not necessarily stored or processed on the devices themselves. The inevitable reality we’re already beginning to witness is that a device equals access—a key that unlocks the wealth of information and processing power that lies beyond. Log in and get started. It will be that simple. Data synchronized and updated in real time. Programs are patched, enhanced, and updated without the need to distribute, license, download or install. The cloud does that.

2. See supra note 1.
3. Id.
Of course, while every cloud has a silver lining, clouds may have a dark side as well. The Cloud Computing Task Force at Reed Smith will be presenting a series of articles (of which this is the first)—collectively entitled “Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing” to tackle both the opportunities and the dangers, i.e., the risks and the rewards. This series will approach the legal issues and implications a little differently from traditional law review articles. While much that has already been written about cloud computing concerns itself with data protection, privacy and security—and we will address these issues as well in what we believe will be a more global and comprehensive manner—this series of articles also will cover cloud computing issues you may have heard little about, but that are and will be no less significant.

Cloud computing promises great advances in the use of technology by individuals, restoring the power of individually-driven communication, creation, collaboration and distribution both to and from individuals, no longer constrained by the need for expensive devices and complex connections. The consumer, the employee, the gamer, the student, will have individualized access to tools and capabilities unheard of even by today’s standards. That said, if you can’t get to the Internet, or if current bandwidth is strained and unable to carry the traffic, you could be tapping your toes in frustration, waiting while an important document or the collaboration over a file is waiting. While this migrates and evolves, will we still need backup on our devices and, if so, doesn’t that defeat the whole purpose? Or can contracts, service levels, requirements and agreements protect you? Do you have insurance to cover these situations? Does your provider? The cloud revolution will create new capabilities, new opportunities, new challenges and new providers seeking to fill those needs. Cloud computing will also create new economic and business models, as well as new economies of scale.

It is likely that cloud providers will figure out security standards, and while no data protection scheme will ever be perfect, so much has been written and voiced about the issue that it would be hard to imagine that this, along with simply building the necessary infrastructure, is not at the top of the agenda for interested parties. But because cloud computing is really more a business and process model, rather than a technological innovation, there are a host of issues that are arising and will continue to arise from this dynamic shift in business processes emanating from cloud computing.

Is a public cloud sufficient for your business or do you need a private cloud—or both (also known as a hybrid cloud), depending on the particular requirement? Corporate technology spending probably will move from capital equipment or licensing to subscription, usage or demand-based pricing, much like a utility, but possibly segmented by complexity of application, intensity of storage and retrieval requirements, and driven by capacity during peak rather than weak usage periods. What about cloud service providers? There are concerns about performance, recovery, and security, as well as availability, which suggest two points little spoken about these days among the legal community: standards and interoperability.

Electricity and electrical outlets are almost uniform, but not quite. We still have adaptors and worry about voltage differences across continents and countries. No single cloud provider will be exactly the same as any other, and no single provider is likely to be able to be all things to all customers, everywhere, all the time. But there are currently no standards or any interoperability requirements, at least nothing binding or even accepted on an industry-wide level. One can call from a mobile phone as any other phone in the world—standards, interconnectivity and interoperability built over years of development in conjunction with consumer and commercial demand made that possible. No such standards and no such interconnection requirements exist in the clouds today. Not only will this pose a challenge to commercial customers and users, but it may also result in barriers to entry among cloud providers—after all, infrastructure is expensive and global capability more.

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

A. Importance of the Financial Services Industry

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, are simply 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 information technology (IT) platform.

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 across 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. For example, the Gramm-Leach-Bliley Act of 1999 (GLB Act) 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, also apply to the extent that they impose more stringent security standards than the GLB Act. To the extent an institution, in some cases, one of 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; or 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 also subject to an increasingly complex web of other laws, regulations and guidelines issued by numerous governmental and regulatory bodies, both individually and collectively, such as the Federal Reserve Board (FRB), OTS, OCC, FTC, SEC, FFIEC, and FDIC, and even self-regulatory initiatives such as those developed and implemented by the Payment Card Industry (PCI). As noted below, this litany is now to be joined by the impact of the Dodd-Frank Act.

At its core, 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 realized, after years of failed efforts to stymie this explosive business, that the key to encouraging its growth was to impede the processing of financial transactions. The solution was to tack an Unlawful Internet Gambling Enforcement Act onto the Security and Accountability For Every Port Act of 2006, which President Bush signed into law October 13, 2006.

Of potentially even greater long-term consequence, the financial crisis that began in 2007, coupled with the perceived failure of the financial 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, an autonomous entity housed within the FRB, may be the most powerful federal agency in the United States. The CFPB has a single but very broad mission—to protect consumers. The scope of the CFPB mandate includes the development of consumer protection rules previously within 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 disclosures and consumer protection mandates; and 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.

6. See, e.g., 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 on a “need-to-know” basis.

7. See id. at sec. 5.3.2.1 (August 2009). Requirements include encryption of credit card account data when transmitted, and restriction of access to cardholder data on a “need-to-know” basis.

B. International Implications of Cloud Computing

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 that jurisdiction 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 the 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 borrow a paradigm from the telephone 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 the United States, 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 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 be concerned with the differing foreign laws and regulations governing their operations in every jurisdiction in which they do business—and, in some cases, laws and regulations that are not merely different, but inconsistent. 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 European Union (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.

C. U.S. Law and Regulation

Returning the focus to the United States, issues that financial services firms will be forced to grapple with include outdated and less-than-helpful regulations and laws. By way of example, the Federal Financial Institutions Examination Council (FFIEC) over the past decade has 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 released 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 in 2004, there are others that may 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.” 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 requirements, like FINRA’s Notice on Members’ Responsibilities When Outsourcing Activities to Third-Party Service Providers, issued in 2005, requires National Association of Securities Dealers (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. Even the largest and most capitalized financial services firms will think twice about cloud computing if they are required by a 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?

D. Third Party Service Providers

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 applicable statutes and regulatory bodies, as well as the numerous other regulations and guidance documents, make 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 laws, guidelines and regulations. As far as the regulators are concerned, it will ultimately be the financial services firm’s responsibility 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.

E. Models of Cloud Computing

There are essentially four models of cloud computing environments available to financial services firms—private, community, public and hybrid. The defining characteristic of a private cloud is that it is operated solely for one organization. A community cloud is often shared by several organizations and supports a community with shared requirements. A public cloud is made available to the general public or a large industry group. A hybrid is some combination of two or more of the three other cloud environments—private, community and public.

Private clouds, because they are developed and used solely for the benefit of one organization, provide the most security of the alternative cloud computing 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 in 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 data-protection parameters similar to those 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

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.

F. Operational Issues

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 an information security officer or director and his or 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 client firm should be wary that it does not become a test case for such a service provider and, essentially, end up funding cloud computing research and development. 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

G. Due Diligence Checklist

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

- Determine which business functions might be suitable for different cloud computing 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 computing environment where capacity is available on-demand. On the other hand, functions that involve the collection and treatment of large amounts of NPII may require use of a private cloud, or may not be suitable for transfer to a cloud computing 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 computing environment. It may be beneficial to develop the service level agreement in advance so that all of 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 standards development, audit rights, frequent steering committee meetings, and clear escalation procedures. Considering the relatively nascent state of evolution of cloud computing services, it may be even more critical as compared 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 the robustness of information security, but also how readily the 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.

III. Conclusion

Adoption of cloud computing within the financial services industry is still in its infancy, as evidenced by a 2010 survey of several IT professionals within financial services firms. 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 that:

- thirty-four percent of respondents believe that cloud computing is not strategic to their company, while twenty-six percent of respondents believe their company is risk-averse to cloud computing;

- fifty-eight percent of respondents only plan to invest in essential IT functions, such as security and compliance; and

- more than seventy-five percent of respondents are concerned about increasing government regulation.

While at first glance these statistics provide somewhat of a dark (or at least, as noted, cloudy) 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 must 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 are stretched to the limit. In many cases, cloud computing and related 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 management 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 the firm’s operations.

When asked to explain the survey results, LogLogic 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.12

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


12. 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.
2010–2011 UCC Update

By John Krahmer

I. Introduction

This article describes and analyzes selected recent cases decided under the Uniform Commercial Code (UCC). A few cases decided under other statutes are also included.

II. UCC Article 3: Negotiable Instruments

A. Preemption of Common Law Claims

In *Ross v. Bank of America*,¹ an office manager employed by a Houston podiatrist from 2006 until the early summer of 2009 apparently decided that she was underpaid and proceeded to supplement her salary by diverting checks made payable to her employer. Instead of restrictedly indorsing the checks and depositing them into her employer's account as instructed, she indorsed in blank and deposited at least 150 of the checks into her personal account at another bank. In a subsequent action by the employer against the depositary bank for conversion and for "money had and received," the employer alleged that the depositary bank "systematically failed to notice that the checks [the office manager] deposited clearly bore a special and restrictive endorsement" to other banking institutions, were fraudulently endorsed in blank with [the employer's] signature, were restrictively endorsed to other accounts at other banks, or bore no endorsement at all." The depositary bank moved to dismiss the common law claim for money had and received on the ground that section 3.420 of the Tex. Bus. & Com. Code (UCC section 3-420) preempts such claims. Reviewing earlier Texas cases, the court concluded that section 3.420 does not completely preempt the common law conversion claim, but that recovery on that claim would be limited by the restriction stated in section 3.420 to the face amounts of the checks.²

As to a cause of action for money had and received, a law review article points out that:

> [a]ssumpsit for money had and received has historically been available as an alternate theory of recovery for both payees and, in some states, drawers. When the UCC was enacted, the question naturally arose whether the right of action for conversion codified in [former section] 3-419 would, later, in [revised section] 3-420 displaced a claim for money had and received.

Some courts viewed the claims as virtually interchangeable. Others regarded them as independent. The displacement issue arises in several contexts.

---

¹ 693 F. Supp. 2d 692 (S.D. Tex. 2010).
² The terms "endorsement" and "endorse" are spelled in the plaintiff's petition with an "e" and not with an "o" as used in Article 3. Either spelling can be considered correct. Despite the statutory usage, banks continue to stamp checks as "P.O.E.G. standing for "Passed endorsement guaranteed." As explained in *Perot Corp. v. First Nat'l Bank of Hohenheim*, 537 S.W. 3rd 10 (5th Cir. 1977), "[t]his practice could be attributed to the bankers' understandable reluctance to stamp "Pay any Bank in the State" on the backs of the checks they handle."
³ Tex. Bus. & Com. Code § 3.420(b) provides: "In an action under Subsection (a), the measure of liability is presumed to be the amount payable on the instrument, but recovery may not exceed the amount of the plaintiff's interest in the instrument."