

Offshore Outsourcing Considerations for Financial Institutions

Contributed by: Talat Ansari, Deepak Nambiar and Jennifer Vickers, Kelley Drye & Warren LLP

For financial institutions, outsourcing of the IT and business process functions to an offshore location has its rewards. But it also implicates regulatory compliance and security risks. This article discusses how a financial institution can mitigate compliance and security risks in an offshore outsourcing transaction while minimizing the institution's regulatory impact.

Regulatory Requirements

Before embarking on an outsourcing relationship with a third-party service provider, whether domestic or foreign, financial institutions must make themselves aware of the regulatory requirements imposed on such relationships. Failing to comply with these requirements can subject a financial institution to fines and penalties.

For instance, the Bank Service Company Act and the Home Owner's Loan Act require a financial institution to inform the relevant federal agency within thirty days of entering into a contract with a third-party service provider. This facilitates the agency's access to critical information related to the servicing relationship and ensures compliance with U.S. laws.

The Bank Secrecy Act, which is designed to keep financial information secure by regulating how financial institutions report and document financial transactions, places costly reporting requirements on financial institutions in offshore outsourcing relationships. For instance, the Bank Secrecy Act requires financial institutions to make financial transaction documents and reports available to regulating government agencies upon request, even if those documents are maintained overseas.¹ The Patriot Act has even more stringent reporting requirements, requiring that financial institutions make anti-money laundering compliance data available within one-hundred and twenty (120) hours of the government's request, which can be challenging when the information is in another country.²

Another law affecting the relationship between foreign service providers and financial institutions is the Gramm-Leach-Bliley Act (GLBA). The GLBA imposes obligations on financial institutions to protect consumer information from internal and external security threats. At the outset of an outsourcing relationship, financial institutions

© 2010 Bloomberg Finance L.P. All rights reserved. Originally published by Bloomberg Finance L.P. in the Vol. 3, No. 7 edition of the Bloomberg Law Reports—Banking & Finance. Reprinted with permission. Bloomberg Law Reports[®] is a registered trademark and service mark of Bloomberg Finance L.P.

The discussions set forth in this report are for informational purposes only. They do not take into account the qualifications, exceptions and other considerations that may be relevant to particular situations. These discussions should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Any tax information contained in this report is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. The opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content contained in this report and do not make any representation or warranty as to its completeness or accuracy.

must contract for service providers to implement appropriate security controls, as required by law, in handling consumer information. But GLBA obligations do not end at contracting. The GLBA also requires financial institutions to continuously monitor, for the life of the outsourcing relationship, their service providers' activities to ensure that they are properly protecting consumer information. While the GLBA enhances information security measures, it can be costly for a financial institution to comply with the contracting and oversight requirements, particularly when contracting with a foreign service provider.

More recently, the federal government enacted the Secure and Fair Enforcement Mortgage Licensing Act of 2008 (S.A.F.E. Act) to further protect consumer information and privacy and to make it easier for the U.S. to regulate all mortgage originators. The S.A.F.E. Act requires all individuals who perform mortgage origination services to acquire a license. Even though the S.A.F.E. Act is a federal law, it requires that each state implement its own mortgage origination licensing requirements. Because the S.A.F.E. Act requires that independent contractors who perform loan processing and underwriting services have a license, financial institutions that outsource their mortgage origination services must ensure that their service providers also obtain a license.

Privacy Concerns

Consumer privacy and data protection concerns are not limited to regulatory compliance. Data security breaches by offshore service providers can result in significant legal and operating costs, as well as crippling losses to a financial institution's credit and or reputation. These risks may vary based on the type of business model or type of services for which the parties contract. Financial institutions can mitigate the risk of third-party data security breaches through proactive contracting and by diligently monitoring the service provider's processes and controls.

Before contracting against potential liability from a data security breach, an institution must understand the amount of risk involved in the service arrangement. For instance, outsourcing information technology services like application development and maintenance run a lower risk of security breaches, whereas, outsourcing business process services such as mortgage services and consumer help desk services greatly increases those risks. Similarly, outsourcing to foreign subsidiaries imposes less risk than outsourcing to a third-party service provider. But the riskiest business model is outsourcing directly to a foreign service provider or outsourcing to a domestic service provider who then subcontracts the work to a foreign service provider. This form of offshore outsourcing renders a financial institution the most vulnerable because the financial institution may have very little control over the integrity of its consumers' data.

Even the most secure forms of offshore outsourcing necessitate well drafted service agreements to protect all parties from loss and ensure the business relationship works at an optimal level. The terms of the service agreement facilitate safeguarding consumer privacy and information. Because U.S. companies can be held liable under state and federal unfair and deceptive trade practices law for not complying with their own security and data protection policies, the service agreement should require the service provider to comply with the financial institution's data security policies

and architecture requirements. Furthermore, to ensure compliance with this provision, a financial institution should conduct periodic audits, including detailed security audits.

Despite a service provider's best efforts to follow a financial institution's data protection and security policies, all companies are vulnerable to security breaches. Therefore, financial institutions should require service providers to immediately notify them in the event of a security breach. More importantly, financial institutions should consider including indemnification and limitation of liability provisions in their service agreement. These provisions indemnify the financial institution from third-party claims arising from confidentiality, security, and data protection breaches by the service provider. That said, financial institutions should be mindful that such indemnification provisions may not be enforceable under the laws of the country where the foreign service provider is located.

Financial institutions should also obtain sufficient insurance coverage to protect themselves from liability. In addition to self coverage, the service agreement should require foreign service providers to maintain adequate insurance coverage for third-party data breaches or any other loss arising from the services provided. Service providers should also be required to notify the financial institution of any material changes in insurance coverage.

In addition to domestic privacy concerns, U.S. financial institutions must be equally aware of foreign privacy laws which may be more stringent than U.S. law. For instance, the European Union enacted comprehensive privacy and data protection legislation entitled the Data Protection Directive. The Directive places strict requirements on any institution or person who collects or processes a consumer's personal or professional information.

Intellectual Property

Intellectual property is a complex issue for domestic service providers, but, similar to privacy laws, it is further complicated when outsourcing services to a location outside the United States. Intellectual property rights vary greatly by country, and may not afford companies outsourcing their IT and business functions to foreign countries the same protections available under U.S. law. Financial institutions should educate themselves regarding local intellectual property laws in order to draft service agreements in such a way as to optimize their property rights over data, copyrights, patents and trademarks.

In order to properly protect consumer information, a financial institution should include a contract provision allowing it to maintain complete ownership of any data transferred to the service provider regardless of how the provider processes, manipulates, or stores the data. The provision should also require the service provider to return the data immediately upon request or termination of the services provided. The financial institution should also include a contract provision to determine who owns any work product developed by the service provider, including design, graphics and software code.

Choice of Law

As described above, contracting is the best way to mitigate the risks financial institutions face when outsourcing their business services overseas. But once a dispute arises, which law should govern? Determining whose law applies will affect the continuity of service, access to data, and protection of consumer information. Thus, a financial institution must be careful to consider whether U.S. or foreign law should govern the service agreement.

Many financial institutions may prefer to apply U.S. law. But even if U.S. law is optimal and it applies pursuant to a valid choice of law provision, a U.S. judicial award may not be enforceable in some countries.

In order to avoid the enforceability issue, a financial institution should consider including an arbitration clause in the service agreement. Arbitration is preferable in countries that are members of the New York Convention because a member country will generally enforce a U.S. arbitral award.

Conclusion

Before entering into a relationship with a foreign service provider, consult with counsel regarding risks associated with outsourcing services to a foreign location and how to mitigate those risks.

Talat Ansari is a partner with the law firm of Kelley Drye & Warren LLP where he heads the Firm's India practice group.

Deepak Nambiar is a senior associate with Kelley Drye's technology and India practice groups, with extensive experience in cross-border technology licensing, outsourcing, and corporate transactions.

Jennifer Vickers is an associate with Kelley Drye, focused on regulatory compliance and insurance recovery matters.

The authors can be reached at tansari@kelleydrye.com, dnambiar@kelleydrye.com and jvickers@kelleydrye.com.

¹ Federal Deposit Insurance Corporation, Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers, FIL-52-2006 (June 21, 2006).

² *Id.* at note 3.