Practical Considerations for Financial Privacy Compliance in Cloud Computing Arrangements

By Blanche Stovall

This article addresses financial privacy considerations when entering into cloud computing arrangements. It includes guidance on key points to consider when conducting due diligence on potential cloud service providers and pitfalls to avoid when negotiating contracts.

The cloud is attractive because of its cost savings and agile business models, but along with these benefits come unique challenges. The same basic rules that apply to any outsourcing scenario also apply to cloud computing arrangements. Due to the nature of the services, however, cloud computing may require nuanced provisions and more robust controls.

The Cloud

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction."

More simply, cloud computing is the delivery of IT services through a new channel. Instead of doing the job yourself, you are getting someone else to do it for you.

FFIEC Guidance

The Federal Financial Institutions Examinations Council (FFIEC) issued a joint interagency statement in July 2012 (the Cloud Statement) which affirmed that the fundamentals of risk and risk management defined in the *FFIEC Information Technology Examination Handbook* (IT Handbook), especially the Outsourcing Technology Services Booklet ("Outsourcing Booklet") apply equally to cloud computing.

Financial Privacy Laws

Financial institutions must comply with various privacy laws that that generally require the protection of customers' "nonpublic personal information" (NPPI), and limit the authority of financial institutions to share that information with third parties.

The Gramm-Leach-Bliley Act (GLB), which addresses collection, disclosure and safeguarding of NPPI, requires financial institutions to:

- provide an annual privacy notice to customers explaining how their data is maintained and shared, as well as steps taken to protect it, and to provide customers an opt-out process (Financial Privacy Rule), and
- implement an information security program (the Safeguards Rule).

15 U.S.C. § 6801, et seq. and 16 C.F.R. § 313

GLB applies not only to financial institutions governed by the federal banking agencies, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission, and state insurance authorities, but also to companies that are "significantly engaged" in providing financial products and services; including, for example, mortgage brokers, nonbank lenders, and credit reporting agencies that receive information about the customers of other financial institutions.

The Fair Credit Reporting Act (FCRA) restricts disclosure of a consumer's financial and other identifying information and specifies the information that can be included in a consumer's credit report and

the circumstances in which agencies or organizations can be provided with this information. *15. U.S.C. § 1681 et seq.*

The Fair and Accurate Credit Transactions Act (FACTA) added new provisions to the FCRA, requiring certain financial institutions and creditors to adopt an identity theft prevention program designed to detect, prevent and mitigate identity theft by indentifying "red flags." *Sec. 114, 15 U.S.C. 1681m(e).*

State laws. Forty-six states have laws requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

International laws. A number of countries, including European Union (EU) Member States and certain countries in North Africa, the Middle East, Latin America, and Asia, restrict the transfer of individuals' data outside their boundaries *See EC Data Protection Directive 95/46/EC and Practice Notes.*

SEC rules. In addition to the above laws, which focus on access, the SEC imposes requirements on broker-dealers to retain customer information and to supervise and oversee customer communications and other activities. *CFR 240.17a-3.; 17 CFR 240.17a-4***.** Hosting this information on external platforms, such as virtual data rooms (e.g., Salesforce.com, Dropbox.com), makes this requirement more challenging.

The common theme is that that the financial institution will not have full control over its data in a cloud computing arrangement, but still has the responsibility to ensure that vendor activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations.

Maintaining Financial Privacy in Cloud Computing Arrangements

Lack of transparency and control are the key challenges a company faces when outsourcing certain activities or processes to the cloud. The financial institution is accountable to its customers for maintaining privacy and safeguarding information, and must demonstrate compliance with applicable laws to its regulators. The reality of the cloud is that a financial institution may not be able to achieve the transparency it needs and ability to directly control the data in a cloud computing arrangement.

To minimize these risks, financial institutions should conduct robust due diligence on prospective providers before entering into any cloud computing arrangement. If the provider does not instill confidence that personal and other sensitive data are adequately protected, move on.

While a contract cannot cover every contingency or provide complete security, a well-written, comprehensive agreement with detailed service level agreements will help financial institutions anticipate risks, minimize exposure and better protect the customer. It is essential that any agreement clearly outline who controls the data, what activities and processes are covered, and grant the financial institution monitoring and audit rights.

The following points incorporate key elements that should be addressed in a cloud computing arrangement:

Due Diligence

- **Data classification.** Install controls, such as encryption, to ensure customer NPPI and other data whose disclosure could harm the financial institution or its customers is appropriately protected.
- **Data segregation/isolation.** If the financial institution's data is being transmitted over networks or stored on servers along with other clients, the provider should have controls in place to ensure integrity and confidentiality of customers' data.
- **Recoverability.** The financial institution should ensure that its disaster recovery plan addresses cloud formats, the cloud provider's disaster recovery and business continuity plans, and ability to maintain communications. While cloud insurance may provide monetary compensation, it cannot bring back data that is permanently lost.

Vendor Management

- **Knowledge of financial services industry legal and regulatory requirements.** If the cloud provider cannot implement processes to meet regulatory requirements and keep up with the changes, find another vendor.
- **Disengagement.** Contracts and service level agreements should be clear as to:
    - **Data ownership.** The financial Institution needs to maintain control of its customers' data.
    - **Data location.** Servers could be located in numerous locations around the world. Some areas, such as the EU, put additional restrictions on the use and movement of individuals' personal data. Agree in advance on the locations where data may be stored or processed.
    - **Data format.** If the data cannot be read by the financial institution, it is useless. Ensure that whatever format the cloud provider is using is readable and usable by the financial institution, and that any changes to format are agreed to in advance.
    - **Dispute resolution.**

Audit

- Shared environments and virtualized technologies present unique evaluation challenges. Internal auditors may need to enhance training and add staff with expertise in this area. The financial institution should vigorously exercise its rights to monitor and audit the activities of the cloud provider.

Information Security

Continuous monitoring may be necessary in high risk situations in order to ensure that the provider is maintaining effective controls.

- **Data classification/inventory.** Multi-tenant clouds increase the need for data protection and controls to restrict tenant access to their respective data only. The provider should encrypt the data and give additional assurances as to data handling/segregation procedures, and adequacy and availability of backup data.
- **Security incidents.** Storage in the cloud could increase the risk and severity of a data breach. Management processes should include:
    - monitoring of security-related threats and events on both the financial institutions' and provider's networks;
    - thorough incident response methodologies; and
    - appropriate investigation and evidence collection strategies.
- **Data destruction.** In a cloud computing arrangement, there may be a higher risk of data not being completely removed or deleted from a provider's storage media at the conclusion of a service contract. Before entering into the relationship, the financial institution should ensure that the provider can remove all NPPI from all locations where it is stored.

Legal, Regulatory and Reputational Consideration

- **Ability to impose security and privacy requirements.** Contracts should clearly specify the provider's obligations regarding the financial institutions' responsibilities for compliance with privacy laws, responding to and reporting security incidents, and for complying with regulatory requirements to notify customers and regulators in the event of a breach.
- **Subcontractors.** While difficult to monitor, agreements should assure that a provider's subcontractor maintains appropriate levels of data protection.

Location

- **Data transfer.** Although obtaining these commitments may be easier said than done, in jurisdictions that limit the transfer of individuals' data, consider negotiating geographic limitations on where the cloud provider may store customer data, or obtain appropriate promises that the cloud provider will comply with legal restrictions applicable to the financial institution with respect to its customer data.