



# Navigating Data Security

Understanding the impact that new data security regulation has on delivery models like cloud computing is essential today.

**WHILE OTHER REGULATORY**, compliance and legal issues such as the new RE-SPA changes have been the focal point within the primary and secondary mortgage industry over the last year, one issue flying under the radar for many lenders is privacy and data security. Financial institutions are being forced to confront a host of actual and prospective new privacy requirements as a result of new regulations adopted on the federal and state level as well as pending privacy legislation in Congress. With an understanding of these strict requirements, financial institutions that are considering or utilizing the SaaS model delivered through a multitenant cloud architecture must have clear and concise policies that detail how they are complying with the various data security and privacy requirements imposed upon them under federal and state law. Specifically, financial institutions must detail where their consumer's data are, what specific security protections are in place and whom may, or may not, have access to this data.



For registered investment advisors, investment companies, broker-dealers and registered transfer agents, Regulation S-AM addresses data privacy concerns surrounding affiliate marketing through the use of consumer information by providing a "notice to consumers" and opportunity for consumers to "opt-out" of the use of the consumer's information by an affiliate of the SEC registered entity, effective June 1, 2010. Also effective on this date, the extension of the Federal Trade Commission enforcement deadline for Identity Theft Red Flags Rule, as promulgated under the Fair and Accurate Credit Transactions Act, requiring many financial institutions and creditors to adopt written programs as applicable under the rule. In addition, banks and other financial institutions now have the option of using a new model privacy notice to inform customers about their privacy and

information sharing practices. Firms electing to use the new model privacy notice form shall receive the benefit of the model forms' regulatory safe harbor.

As a means of working toward and establishing a more uniform federal data security standard, the House of Representatives passed the Data Accountability and Trust Act (H.R. 2221). This bill would require each business engaging in interstate commerce owning or possessing electronic data containing personal information or contracting with a third party to maintain such data to establish extensive data security policies and procedures. Some of the highlights would require an officer responsible for the information security oversight, vulnerability testing of the security programs, and a process for disposing of electronic data containing personal

information. This legislation, if signed into law, would generally pre-empt the various state data breach notice laws that currently exist and would create a single standard that would most likely be embraced by many businesses that currently engage in interstate commerce. The Senate is currently working on a similar bill, so it is safe to expect that in some form by the end of the year, the federal government will provide additional requirements.

Compounding this issue is the fact that the mortgage industry is turning to Software as a Service and Infrastructure as a Service models that are delivered through a multitenant cloud architecture to eliminate prolonged implementations, reduce the

Financial institutions **are being forced to confront** a host of actual and prospective new privacy requirements as a result of new regulations adopted.

cost of the IT infrastructure, increase scalability options and to better respond to current market conditions. While these solutions definitely have their place in the mortgage industry, it is another reason that more attention needs to be placed on data security and privacy. IT outsourcing requires significant data security and privacy controls to protect consumer data and IP including trade secrets. Lenders, compliance officers and IT staff need to understand how to navigate and keep up with these constantly changing regulations to ensure that their organizations properly address these legal and regulatory standards or face the potential for strict enforcement. This includes the standards to which they hold their IT outsourcing providers who deliver cloud models.

The basic requirement to provide “reasonable security” by providers

of data retention (control, possess, store, transmit and/or process) is not sufficient to address all of the risk concerns that a third-party provider handling data from all states faces. Lenders need to challenge their providers and the provider’s specific “reps and warrants” to address a level of “security” that shall meet all of the applicable privacy and data security laws and regulations beyond current industry standards such as SAS-70 Type II.

Lenders and service providers may need to look outside the traditional arenas for additional best practices for data privacy and security. BITS is a not-for-profit, CEO-driven financial service industry consortium made up of 100 of the largest financial institu-

tions in the US. BITS provides intellectual capital and fosters collaboration to address emerging issues.

To manage risk and respond to the evolving regulatory requirements, BITS created a program called Shared Assessments ([www.sharedassessments.org](http://www.sharedassessments.org)) to assist in the evaluation of the security of the controls that service providers (i.e., vendors providing technology platforms to lenders) have in place. Shared Assessments is a member-driven, industry-standard body that provides all parties a standardized, consistent, faster, more rigorous, more efficient and less costly means of conducting security, privacy and business continuity assessments. More and more, corporations of all sizes are using outsourced services to support critical business functions. But while companies can outsource sensitive data processes and services, they can never outsource responsibility for the

associated risk. To manage risk and respond to evolving regulatory requirements, companies must carefully evaluate the security of the controls their service providers have in place.

Lenders need to require their providers to go further to address the poignant industry standards such as looking to organizations like Shared Assessments and how their best practices exceed the baseline requirements imposed by federal and state law. To effectively address today’s standards and future standards, lenders must have a better understanding of how their providers are handling specific concerns such as:

- Backup and recovery
- Data location
- End user access
- Intrusion detection
- Investigative support
- Personnel issues
- Physical security
- Privileged user access
- Regulatory compliance

These are all concerns that will identify the veracity of the provider and the provider’s ability to effectively handle the data privacy and security of their data. The regulatory landscape is constantly changing as are technology solutions like SaaS and cloud computing. While data privacy and security may not be the most talked about regulatory concern, it does deserve strong consideration and review by lenders, compliance and IT staff. **MT**

---

*John Levonick is the chief legal and compliance officer for Mortgage Cadence and is responsible for working closely with Mortgage Cadence clients in identifying and managing compliance risk. In drawing from his advisory experience, Levonick assists clients in interpreting compliance requirements, developing risk mitigation strategies and implementing the requisite controls within the Mortgage Cadence platform(s) to best protect the individual client.*