

MCIF Database Security – Questions to Ask When Assessing MCIF Providers

By Rich Weissman, DMA

Security is a critical component in the selection of a marketing customer information file (MCIF) provider. Most institutions select providers based on the details of the analytics that the system provides, the functionality of and access to the system, and the level of ongoing support given by the provider. These are all important factors, but must be considered in conjunction with database security.

The trend in cloud computing is to have MCIF systems processed and managed externally. This enlightened approach provides the bank with far greater options and greater skill levels that would not be available internally for most community and regional banks. Not having to process, manage, and support the MCIF internally is a significant step forward for most banks. By utilizing cloud technology, where the system and the data reside externally, assessing provider security is critical. Not to worry, there are ways to ensure that the MCIF system is delivered through cloud technology in a way that meets the highest security standards.

This includes working with a provider who:

Has maximum network security procedures in place.

There are two general routes cloud technology can take: one is to house the databases on the Internet on a website; the other is to use the Internet for data transmission only where the database is housed securely at the provider's data center. We believe that the latter is a more secure method, and this should be a requirement for selecting an MCIF provider. The questions you should ask are: Where is the database housed and what security procedures are in place to ensure that it cannot be accessed by anyone other than the designated bank employees? Does the system require encrypted data transmission? Is access only available to bank employees behind the bank's firewall and how is the provider's firewall secured at its end? Are items such as registration of IP addresses, user names and strong passwords, encryption of at-rest data, etc. part of the normal procedures of the provider?

Has detailed physical site and data center security procedures in place.

It is important that the provider's physical facility be secure, where the data center is secured separately. We believe that having buttoned-up security for the physical site is a critical component, including advanced alarm and surveillance monitoring systems, bio-metric locking mechanism, and dual control access. The questions you should ask are: How is the facility configured for maximum security? How is the data center secured separately? How are dual controls maintained?

Has detailed background and security checks on its employees.

Having the providers' employees go through extensive checks is a critical piece of the equation. We believe that having a base of employees who have been properly scrutinized and trained is an important requirement for selecting an MCIF provider. The questions you should ask are: What steps have been taken to screen provider employees? What kind of data security training have the employees been given?

Has detailed disaster recovery and business continuity procedures in place.

It is also important that the provider can continue operations in a secure manner, without interruption, in the event of a disaster. We believe that a quality provider should have complete disaster recovery and business continuity plans in place, and tested regularly. The

questions you should ask are: What are the back-up/co-location sites and are they outside of the provider's normal operating region? Are the facilities for co-location equally secure as the provider's normal operating site? Are the back-up plans and systems tested quarterly?

It is critical that the provider offer system access on 24/7 basis, so that the bank is never without access to its MCIF. And it is imperative that the MCIF system provides for internal bank administrator to determine user rights and access, with the ability to cut-off any bank employees at any time. Finally, you should only be considering an MCIF provider that has successfully completed SAS 70 Type II audits year-in-year-out, along with other 3rd party industry security audits.

All of these questions and points should be part of your due-diligence when selecting an MCIF provider. Our advice: only select a provider that meets all of them.

Rich Weissman is president & CEO of DMA, headquartered in Beaverton, Oregon. DMA is a leader in integrating technology and sales management. He can be reached at rich.weissman@DMAcorporation.com or 503-597-0088.