

## Addressing Insider Threats, Cyber Attacks & Data Security

Your customers trust you. Protecting their personal information is crucial to maintaining their loyalty. So is acting quickly and efficiently in potential fraudulent situations. Relying on inefficient spreadsheets leads to time-consuming and disorganized investigations that are frustrating for customers.

An enterprise content management (ECM) solution should be a one stop "holding tank" for all of your business critical information. But it's not enough to just have a place to store files and data. An ECM solution should allow for the sharing of that data when appropriate, and the protection of that data at all times. An ECM solution that integrates strong workflow and case management capabilities gives an organization effective information management capabilities without being a hindrance to the business processes that rely on that data. For example, fraud management solutions allow investigators to easily log, access and interact with the critical data involved in a fraud investigation. Leveraging an ECM case management solution for fraud investigations gives employees a 360-degree view of all case-related information – including data records, documents, forms and history. The right case management solution allows banks to act quickly by:

Simplifying the entry, organization and reporting of information surrounding a fraudulent case file

Providing instant and simultaneous access to case files for multiple users

Streamlining investigations with easy access to information from disparate systems with advanced search capabilities

With today's growing internet-based product and service offerings, all financial institutions are at risk of cyber-crime. As technology continues to advance and become more sophisticated, so do the hackers. Unfortunately, there will never be a full proof method that will mitigate 100% of the potential breaches. I think we will continue to see any number of new viruses, worms, etc. leading to additional data breaches. But I think banks have always prioritized the protection of their customers and their personal financial information. They will take the necessary steps to maintain their customers' trust. It's challenging to predict what may be on the horizon when it comes to cyber threats because hackers are diligent too. It will be a never ending battle of ensuring that the bank has the appropriate controls in place to mitigate the security risks that exist. Keeping up with technology is key. Having systems that are up to date is key. DILIGENCE is key!

ECM systems, by nature, are designed for the purpose of protecting sensitive files and data. The value that an ECM solution brings is that the information resides in a single repository instead of multiple silos. This gives banks tighter security that is controlled from a single source. However, simply implementing any old ECM system will not inherently provide the protection and compliance that financial institutions need. Other factors need to be considered when looking for the right solution.

For example:

How granular can security be defined, and who ultimately has control over establishing those security definitions?

Does the solution offer encryption capabilities for information at rest as well as in transit? If so, what kind of encryption is being used (this is a critical consideration for PCI compliance)?

How are access controls and authentication defined and managed?

Is the solution sophisticated and flexible enough to allow the institution to uniquely define and control business processes according to their own policy definitions?

A solid, complete ECM solution will address these issues (and many more). But it can't stop there. In today's world, more business is happening in a virtual manner, which presents a need for banks to share information with customers, vendors and other organizations outside the bank's firewalls. An ECM system that has fully integrated enterprise file sync / share (EFSS) capabilities is a huge advantage to an organization.

Today, vendors like Box.com and Dropbox have been the go-to players for these types of collaborative sharing applications. The disadvantage is that these solutions are separate from your ECM application, where the critical info lives (and should stay), so the security controls when sharing information may not fully sync with the required security established in the ECM solution. An ECM solution that offers an integrated EFSS application changes the game when it comes to file security. With a solution like this in place, documents and data are fully secured, whether they are being accessed internally by bank staff or being shared with external parties.



**Steve Comer**  
Manager, Financial Services

**OnBase**  
by Hyland

### Contact Info

[www.onbase.com](http://www.onbase.com)  
440-788-5810

**Steve Comer** is the Director of Financial Services at Hyland Software, Inc., the developers of OnBase. As the industry director, Comer is responsible for developing sales, marketing and product strategies that help financial institutions drive efficiency and streamline their internal business processes, resulting in faster ROI and increase levels of overall member satisfaction. His team also cultivates and manages relationships with core banking providers and other technology partners to bring added value to financial institutions. Integrating with everyday business applications, OnBase provides instant access to critical information when you need it, wherever you are. It is tailored for departments and comprehensive for the enterprise.