

Addressing Insider Threats, Cyber Attacks & Data Security

Understanding your employees often starts with understanding their work product. One significant challenge that any manager has is establishing appropriate levels of process oversight, and maintaining the integrity of those processes. By applying electronic documents and automated workflow technology across the enterprise, managers and executives gain transparency not only into the flow of documents, but also into who touches each document, what action is taken, when and how it is routed next. Providing an audit trail that captures each step of a transaction creates historical accountability for all of those involved. Specific to IMM's workflow technology, audit trails are automatically collected and archived along with the completed documents for future retrieval.

IMM's bank customers have found workflow solutions critical to controlling processes by establishing policies and procedures for all transaction types to make certain standard operating procedures and regulations are followed properly. This foundation of protection is now largely extended to eSignatures as a step in the process. The latest authentication technique enables users to verify that remote consumers prior to viewing documents are in fact who they say they are. This check and balance is typically performed for each document recipient and signer to protect the non-public private information. Once documents have been complete, they are encrypted or tamper-sealed to protect them from being altered post completion. These provisions aid in any potential insider threats from any employees, vendors, and contractors alike.

The reality is that anything can be breached or hacked. When barriers are placed in one area, attackers will eventually go elsewhere. The real problem facing banks is not on the protections side, but on the side of consumer convenience—how much inconvenience will a consumer accept to avoid being hacked? There are options available today that make it very difficult for attempted hackers to get a hold of the data they seek, but these oftentimes come at a price. Creating a balance between customers' access and ease of use is critical for consumer consumption.

Banks are only as secure as the individuals that have access to their confidential information. Most financial institutions become targets of cyber threats because an employee, advantaged user or trusted third party lacks awareness to their vulnerability; this is most often caused from endless Internet access and the increase in social media use. The level of security a bank wishes to invest in today has become an important decision. IMM allows for in-branch transactions to stay behind the firewall, and only when a customer is remote to securely send that transaction out for review and eSignature. But even then, IMM still offers banks the opportunity to be as secure as they choose with many authentication options.

We receive the most inquiries from banks related to the security of remote eSignatures. During any remote signing event, any data delivered into the cloud from the bank is done in via a secure API with encryption. Whether the data is at rest or in motion, there is encryption. IMM even goes so far as to prevent access to specific sites and information for IMM employees without consent from the bank client.

IMM's TotaleAtlas automates the entire process in which customers eSign exactly where they need to and are not able to complete without all required signature fields. The completed documents contain electronic audit trails and are directly stored into your imaging system, making them safer and consistently prone to less human intervention. The eSignature aligns with legal industry standards, and also has the ability to be controlled to correspond with the established business rules and operating procedures. In many ways, we're helping banks relieve themselves of the burden that data and file security have to be complex at all.



John A. Levy
EVP and Co-Founder



Contact Info

www.immonline.com
Phone: 800.836.4750

John A. Levy is the executive vice president of IMM, a company specializing in paperless technologies that improve a financial institution's transaction process by automating the space between its core host system and imaging backend, including digitized signatures in-branch or remotely. His core responsibilities at IMM encompass overseeing the day-to-day operations of the sales, support, development, quality assurance and design teams. Levy's vision for IMM is to continue to be the leader in delivering quality software to the financial industry that increases productivity and reduces operating costs by streamlining the typically paper-centric financial institution output processes. Teamwork, excellent service and the development of a strong infrastructure are the foundation of Levy's daily operating style.