



# White Paper

---

## **DIGITECH SYSTEMS AND THE FINANCIAL SERVICES MARKETPLACE**

August 2007

The Federal Financial Institutions Examination Council affirms that information is one of a financial business' most important assets. The protection and security of information assets is necessary to build customer trust, maintain compliance with the law and protect the company reputation. A financial business could potentially be ruined if information is shared with unauthorized parties, inappropriately altered or not available at a moments notice.

In the financial services marketplace, information security, reliable recordkeeping and regulatory compliance are core elements of a solid financial foundation. Digitech Systems, Inc. provides Enterprise Content Management (ECM) solutions that enable financial services companies to maintain protected records, to provide secure access to documents and to adhere to government regulations.

## Overview

***“More and more, technology is playing a crucial role in financial services. Customers have begun to make decisions on which institutions they will patronize based on the technology available, so IT takes on such strategic importance that you really can’t ignore it.”***

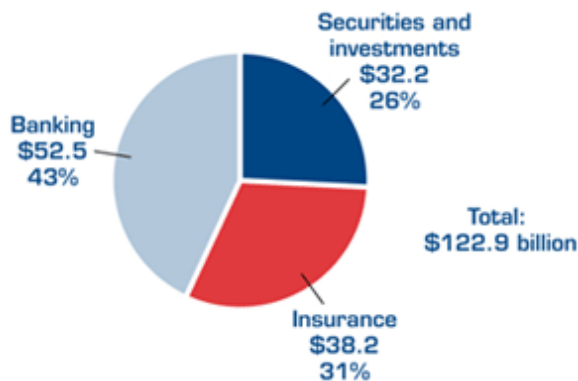
***~Octavio Marenzi,  
Celent  
Communications***

In terms of earnings, the financial services industry is one of the largest markets in the world. It encompasses a wide variety of businesses and services including banks, securities firms, insurance companies, mutual fund organizations, investment banks, pension funds and mortgage lenders. Studies from the U.S. Department of Commerce Bureau of Economic Analysis show the assets of the financial services industry now exceed \$49 trillion.

Information Technology (IT) is critical in the industry. "More and more technology is playing a crucial role in financial services. Customers have begun to make decisions on which institutions they will patronize based on the technology available, so IT takes on such strategic importance that you really can't ignore it," Octavio Marenzi, Managing Director of Celent Communications, told BankTechnologyNews.com.

The information age, the internet and the speed of conducting business electronically increases dependence upon constantly updated technology. IT spending grows as it plays a larger part in providing efficiency, reducing labor costs, online services and increased competitive advantage.

**U.S. FINANCIAL SERVICES INDUSTRY IT SPENDING BY SECTOR, 2006**



Source: TowerGroup

Software and server expenses can be substantial for financial institutions, and studies show spending is increasing. Frost & Sullivan’s vertical market studies anticipate software and consulting/system integration to offer the best potential for organic growth. The Gartner Group studied IT spending in 2006 and determined that the financial services industry was the top spender on computer servers, accounting for 25% of worldwide server sales.

Why are financial institutions spending on software and servers? Senior Research Analyst at Gartner, Kiyomi Yamada, told InternetNews.com that regulations requiring institutions to store data for long periods of time are the cause of these types of purchases.

As these businesses address compliance concerns, many are upgrading to electronic business processes. As they do, it is imperative that they keep a single information source to manage data across all systems and make it searchable and accessible for rapid retrieval. Content management is a fundamental ingredient for success; however, creating secure storage, transmitting sensitive information and implementing an information



management solution (that will not negatively impact existing systems and will actually improve operations) is the ultimate records challenge.

Digitech Systems is committed to providing products that meet the needs of the financial services industry. ECM enables records managers to condense, secure and protect information using a single, searchable source that saves both time and money. Digitech Systems' solution can be scaled to fit any financial institution and enables administrators to enhance operational efficiency.

## Six Principal Concerns when Handling Financial Information

Financial institutions must focus on six principal records issues:

- 1) Information security and confidentiality
- 2) Privacy and protection of personal information
- 3) Records retention in a secure archive with easy retrieval
- 4) Integrity, accuracy and reliability of the document archive
- 5) Audit trails, tracking user activity and document history
- 6) Secure and compliant information disclosures

Since electronic communications have become a primary means of doing business, institutions go to great lengths to deploy self-regulation, information policies, security controls and audits to ensure the security of electronic records. However, financial companies must also maintain security practices that adhere to industry and government regulations.

## Primary Government Regulations

The financial services industry is highly regulated, and compliance presents enormous legal risks for both companies and their officers. Faced with paper-intensive processes and looming regulations, institutions often employ compliance officers solely dedicated to identifying and mitigating risks as well as keeping employees, records systems and procedures in check.

The cost of noncompliance can be tremendous, including fines and even jail time. Therefore, institutions are making significant expenditures to retain records and implement secure information policies. They have spent nearly \$15.5 billion on recent compliance programs, according to a study from AMR Research.

Compared to the average company, financial institutions face a plethora of regulations governing their practices. The list of government regulations that affect their business go on and on, but the following regulations weigh heavily on the industry and specifically dictate what document management practices should be in place.

### Gramm-Leach Bliley Act

The Financial Modernization Act of 1999, also known as the Gramm-Leach Bliley Act or GLBA, opened competition among banks, securities companies and insurance companies and allows commercial and investment banks to consolidate. The GLBA also includes provisions to govern the collection, disclosure and protection of consumers' nonpublic or personally identifiable information; GLBA compliance is mandatory. Whether a financial institution discloses nonpublic information or not—there must be a policy in place to protect information from foreseeable threats to security and data integrity. The following



three rules govern the collection, disclosure and protection of consumers' personally identifiable information.

### Financial Privacy Rule

The Financial Privacy Rule provides privacy policy agreements between the company and the customer and protects the customer's personal, nonpublic information. When the consumer relationship is established and on an annual basis thereafter, institutions must provide each consumer with a privacy notice. The privacy notice must explain what consumer information is collected and how that information is shared, used and protected. Customers must have a right to "opt-out" of the information sharing. If privacy policies change, customers must be notified.

### Safeguards Rule

The Safeguards Rule forces institutions to take a closer look at how they manage personal information and analyze their information policies and systems. It requires them to develop a written information security plan that describes how the company is prepared for and plans to continue to protect customers' (and former customers') personal information. This plan must include the following document management policies:

- Denote at least one employee to manage the safeguards
- Develop, monitor and test a program to secure the information
- Establish flexible and modifiable safeguards that adjust as changes are made to information collection, storage and usage

### Pre-Texting Protection

GLBA provisions require institutions to protect information from unauthorized access—even when someone tries to gain access to personal information without proper authority to do so. This is referred to as "pre-texting," social engineering, fraud, trickery or a scam used to manipulate people into divulging confidential information. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (using a "phony" website or email to collect data).

Digitech Systems' ECM solutions provide the tools institutions need to comply with GLBA through the following software capabilities:

- Multiple security levels and access controls protect personal financial information
- Redaction hides personal information from system users
- Unlimited distribution capabilities allow companies to easily and cost-effectively communicate policies and privacy notices
- Security settings, workflow processes, system auditing and document history reports document how information is shared, used and protected
- Security controls, user access, index fields and system settings are flexible, modifiable and easily adjusted by system administrators
- Encryption both during transmission and when stored protects information from "pre-texting" and electronic intrusions

Plus, Digitech Systems' on-demand solution, ImageSilo, is an affordable option for institutions looking for these comprehensive services.

## U.S. Securities and Exchange Commission

The U.S. Securities and Exchange Commission (SEC) was created by Congress to regulate the securities markets, enforce federal securities laws and protect investors. They are responsible for implementing rulings on requirements for the Sarbanes-Oxley Act (covered in detail later) and dictate several rules that influence document management for financial institutions.

Under the Securities Exchange Act of 1934, SEC Rules 17a-3 and 17a-4 apply to the securities industry and specify records retention policies for publicly traded companies. The SEC, self-regulatory organizations and others may examine institutions' document management systems for compliance. For the past 70 years, the SEC rules covered paper records, but today, they also include electronic files and email. Originals of all business communications, whether by paper, by email or through audit reporting, must be stored on a non-rewritable, non-erasable media that is fully indexed and easily searchable for three years from origination.

Since 1997, the SEC has allowed national securities exchange members, brokers and dealers to store records electronically. The SEC makes detailed requirements for brokers and dealers using electronic storage media. (SEC regulations specific to broker-dealers are discussed in depth later, under the Investment/Securities Industry section.)

Digitech Systems' ECM solutions provide tools to comply with SEC Rule 17 by addressing:

- Backup and storage of information to any media, including non-rewritable and non-erasable media
- Distribution assistance which allows users to send files to any external media
- Capture capabilities index images then export them to any media for preservation
- Email management captures messages and manages them in the ECM system

## Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox, is a federal law passed in response to a number of major corporate and accounting scandals that resulted in a decline of public trust in accounting and reporting practices. SOX mandated a number of reforms for publicly traded companies to increase corporate responsibility, enhance financial disclosures and combat accounting fraud.

SOX programs topped the list for industry compliance spending, accounting for 40% or \$6.2 billion of the \$15.5 billion spent on compliance issues, according to a recent AMR Research study.

In short, SOX requires tight control over significant transactions and financial reports. Institutions must show how transactions and reports were created and be able to identify where misstatements, errors or fraud could occur. Each system that contributes to financial statements, reports and disclosures must be monitored and tracked with audit trails. An internal control report must certify that companies have accepted the responsibility for establishing, evaluating and correcting the security controls. Finally, chief executive officers must sign off on financial reports.

SOX regulations affect document management practices. Both the regulatory body that oversees public company auditors and SOX Section 404 specifically address recordkeeping.

### Public Company Accounting Oversight Board

The Public Company Accounting Oversight Board (PCAOB) oversees auditors of public companies. The PCAOB requires institutions and auditors to:

- Assess both the design and operating effectiveness of internal controls related to financial statement assertions and disclosures, security designed to prevent or detect fraud and the safeguarding of assets
- Understand how significant transactions are initiated, authorized, supported, processed and reported
- Document sufficient information about the flow of transactions to identify where material misstatements due to error or fraud could occur

### Section 404

SOX section 404 mandates that firms listed on U.S. stock markets provide annual disclosures and quarterly updates to shareholders on the effectiveness of internal controls over financial reporting processes. Signing officers must evaluate and document their internal controls and their control deficiencies for SEC review. Published information must state annual reports showing scope, adequacy and effectiveness of the internal control structure and procedures for financial reporting.

Section 404 has been under fire for being too burdensome and too costly for small businesses that will begin to officially comply with section 404 in 2007. Critics have argued that the regulations should be scalable and “proportionate to the complexity of underlying corporate structures.” In April of 2007, the SEC announced it will endorse changes to section 404 that will allow more flexibility in the rules. The new rules are expected to be approved in 2007. (For more information please visit: [www.sec.gov](http://www.sec.gov).)

Paper documents make it difficult to demonstrate control over the use and access of information, which is the primary reason institutions and public companies pursue ECM solutions for SOX compliance.

Digitech Systems’ ECM solutions provide the following tools to enable compliance with SOX:

- Multiple security levels allow companies to control security, access to information and user activity
- Workflow processes permit companies to design and enforce standard document procedures
- Workflow reports, audit trails and activity reports enable companies to understand transaction processes from start to finish and help them analyze the effectiveness of internal controls
- Workflow and audit trails provide detailed information about the flow of transactions, the controls or requirements for transactions or reporting process and user activity at each stage of the process
- Group-level, user-level and document-level security allow companies to establish and verify internal controls
- Printed reports of workflow processes can provide proof for the scope, adequacy and effectiveness of the internal control structure and procedures for reporting

Finding an affordable system that includes needed capabilities but doesn't burden IT staff is a challenge for financial institutions. Digitech Systems' on-demand solution creates an affordable option for companies looking for comprehensive services with minimal IT demands.

## The Banking Sector

### \$60 Billion in IT Spending—Mostly for Compliance Aids

Banking is the largest sector within the financial services industry. Banking includes all depository institutions, from commercial banks and savings banks to credit unions.

Compliance and regulatory issues are critical in the banking sector. Virtually every aspect of banking is regulated by federal and state agencies. To make matters more complex, different types of agencies regulate different types of banks. In fact, under the heading "Most Important Laws that have Affected the Banking Industry," the Federal Deposit Insurance Corporation's (FDIC) website lists 24 different legislative acts that date back to 1864.

Compliance is a driving factor in IT spending. The banking industry is expected to spend \$60 billion on IT in 2007, a 5% increase over spending last year, according to IDC market analysts. IDC studied strategic priorities and the role IT would play in achieving banking goals. The leading priority was meeting regulatory requirements, and the largest share of IT spending will go to services that aid compliance.

### FDIC Regulations

In 1933, Congress created the FDIC, an independent agency of the government, under the authority of the Federal Reserve Act. It was designed to promote and preserve public confidence in banks after the 1929 stock market crash and the Great Depression. The FDIC provides insurance coverage for bank deposits, thereby maintaining financial stability throughout the country.

FDIC technology regulations address everything from money laundering to information sharing, privacy and identity theft. To develop regulations and enforce compliance, the FDIC works with other federal agencies such as the SEC, the Federal Trade Commission and the Commodity Futures Trading Commission. The FDIC conducts IT regulatory examinations, where banks are scrutinized for compliance. The examination programs include risk management, compliance, IT and recordkeeping to prevent money laundering.

Protecting customer information and preventing identity theft are two of the top FDIC hot buttons that directly impact document management. While the FDIC is still developing supervisory policies to minimize identity theft, the Guidelines to Safeguard Customer Information, as mandated by the GLBA, requires banks to address standards for implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information. ([www.fdic.gov](http://www.fdic.gov))

While the FDIC does not dictate specific document management requirements for banks, they expect banks to have written policies and procedures that address the following issues:

- User access controls
- Disaster recovery procedures and tests

***Because banks must reimburse consumers whose credit card data was stolen, they are pressuring retailers to comply with credit card security standards or be held liable for the losses.***

***This is the case between bank executives and a major off-price retailer. In 2005, hackers stole 45.7 million credit card numbers from the retailer, resulting in at least \$8 million worth of fraud and theft.***

- Backup practices
- Security measures including firewalls
- Encryption during transmission and for storage
- Validation methods (audits, security assessment, compliance validation)
- Password control features
- Activity logs and reports
- Controlled system changes

Digitech Systems' ECM solutions provide the tools to comply with FDIC requirements by offering the following capabilities:

- Group and user controls restrict employee access to documents, limit their system abilities and safeguard information from unauthorized access
- Data backup systems deliver file backups at regular intervals, and 256-bit AES data encryption protects data both during transmission and when stored
- ImageSilo provides multiple security levels including firewalls and 24/7 physical and electronic system monitoring
- Document and user history reports, audit trails and workflow reports can be used as proof of internal controls by showing who accessed what, when and why
- Only authorized system administrators can make changes to security settings, so system changes are controlled

### **Banking Sector: Moving to Electronic Processes**

Because banking is an information-based business, the importance of information security and the long checklist of compliance issues drive companies to investigate ECM solutions.

The Office of the Comptroller of the Currency (OCC), a bureau of the U.S. Department of Treasury, issued an advisory letter regarding electronic record keeping. The OCC said an electronic records system must have sufficient accuracy, accessibility, integrity and must serve multiple purposes, such as: litigation support, internal and external audits and controls, bank supervision, regulatory compliance as well as data backup and recovery.

Digitech Systems software provides tools for all of the OCC's above criteria. For example, accuracy is ensured with capabilities such as:

- Capture capabilities verify that data has been scanned properly and images are accurate
- Image cleanup capabilities remove spots and repair misaligned documents to ensure an image is represented accurately
- Version controls make sure users have the most recent information and don't overwrite each other
- Workflow confirms conditions are met before routing documents through specific procedural steps

Secure accessibility is ensured with capabilities such as:

- On-demand ECM provides the convenience of online access while maintaining system securities

- Group-level, project-level, user-level, document-level and function-level security settings govern user information access and permissions to perform specific tasks
- Redaction hides sensitive information from users, while still allowing them to work with the document

System integrity is ensured with capabilities such as:

- Firewall technology protects against electronic intrusions
- Data encryption can occur both during transmission and when stored
- Multiple types of security protect system access and control users and documents
- Enhanced auditing provides document history logs and user reports detailing system activity
- ImageSilo's state-of-the-art data center provides built-in physical securities and simple disaster recovery capabilities

Furthermore, PaperVision Enterprise and ImageSilo enable banks to manage many forms and transaction records in a single source that allows employees to access information quickly and efficiently. These ECM solutions reduce human errors, improve customer service, enable regulations compliance, offer disaster recovery strategies and reduce records management costs.

## ***The Investing/Securities Sector***

---

### **Compliance Costs \$3.2 Billion**

The securities industry consists of brokers and dealers, investment banks and advisers, and stock exchanges. Together, these entities facilitate the flow of funds from investors to companies and institutions seeking to finance projects. Firms that make up the securities sector may specialize in one segment of the business or engage in a wide range of activities that include brokerage, asset management and advisory services, as well as investment banking. ([www.financialservicesfacts.org](http://www.financialservicesfacts.org))

Overall, firms in the securities industry are spending 13% of net revenue on compliance-related activities. They place a premium on compliance, having spent an estimated \$3.2 billion in recent years, according to the Securities Industry Association.

### **NASD Regulations**

The National Association of Securities Dealers (NASD) is a self-regulatory body created by amendments to the Securities Exchange Act of 1934. The organization serves as the primary private-sector regulator of America's securities industry. Under federal law, virtually every securities firm doing business with the U.S. public is a member of this private, not-for-profit organization, according to the NASD.

Editors Note: On July 26, 2007, the SEC approved the formation of the Financial Industry Regulatory Authority (FINRA), a new self-regulatory body that will succeed the NASD. FINRA will consolidate NASD and the enforcement arm of the New York Stock Exchange. For now, existing regulations remain in place, but the new regulatory body may introduce regulatory changes. Although the NASD name is used here, the organization has officially taken the FINRA name. For the purposes of this publication, the two names should be considered interchangeable. Please visit [www.FINRA.org](http://www.FINRA.org) for more information.



In a 2006 Securities Industry Association survey of compliance costs, participants said three NASD rules presented “significant burdens.” These rules are the NASD 3010, 3012 and 3013, which cover written procedures, supervisory control systems and the annual certificate of compliance.

#### Rule 3010: Written Procedures

Rule 3010 states members must establish, maintain and enforce written procedures for communications and ensure compliance with all applicable securities laws and rules. It also requires securities firms to review incoming written and electronic correspondence to identify and handle customer complaints and to ensure that customer funds and securities are handled in accordance with firm procedures.

#### Rule 3012: Supervisory Control System

Rule 3012 requires one or more principals to take responsibility for establishing, maintaining and enforcing a system of supervisory control policies. This person must test and verify that procedures are designed to achieve compliance with the laws. The designated person must submit a report annually to senior management detailing the controls, test results, expectations and any amended procedures. Procedures must review and supervise customer account activity on a day-to-day basis. The procedures must review and monitor the transmittals of customer funds and securities, customer change of address and validation, and customer changes of investment objectives and validation. Customer confirmation must be documented.

#### Rule 3013: Certificate of Compliance

Every member must designate a chief compliance officer who is responsible for executing an annual certification that the firm has processes, procedures and supervisory policies in place that establish, maintain, review, test and modify written compliance. ([www.FINRA.org](http://www.FINRA.org))

Digitech Systems’ ECM solutions provide the tools to comply with NASD requirements by offering the following capabilities:

- When PaperVision® Enterprise WorkFlow is used with PaperVision® Message Manager, email messages from customers can initiate a workflow process to ensure customer requests and concerns are handled properly
- Written requests and business practices can be tracked and audited in a workflow process to ensure compliant procedures
- Multiple security layers enforce information policies and control user activity

### SEC Rule 17: Regulations for Electronic Storage Media

In order for brokers, dealers and members to use electronic storage media, they must have ECM systems that adhere to SEC requirements.

Under SEC rules, the electronic storage media must:

- Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media
- Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable

The broker, dealer or member must:

- Be able to produce easily readable images
- Provide facsimile enlargement upon request
- Store separately a duplicate copy of the records
- Organize and index accurately the records and their duplicates
- Have an audit system for accountability
- Preserve the audit system results
- Maintain, keep current and provide promptly upon request all information necessary to access records and indexes stored

### **Investing/Securities Sector: Moving to Electronic Processes**

Processing securities documents can be a very time-consuming process and human mistakes are costly. Integrating different existing systems is a challenge, and secure information distribution is important because of regulatory risks. Managing information across branch offices and keeping everyone on the same page can be difficult.

Digitech Systems provides brokers and dealers with the tools to effectively secure and manage information and comply with SEC regulations in the following ways:

- Image quality can be assured with PaperFlow™ products
- Image cleanup capabilities remove spots and repair misaligned documents to ensure an image is represented accurately
- Zoom-in capabilities allow enlarged image viewing for faxes and other hard-to-read documents
- Indexing capabilities accurately organize records
- Multiple security levels and data encryption ensure accountability
- Enhanced auditing provides document history logs and user activity reports detailing system activity and facilitating accountability
- Data Delivery and Data Transfer Manager assist customers in storing a duplicate copy of the records
- On-demand access to information improves information accessibility and provides a comprehensive yet affordable solution

## ***The Mortgage and Lending Sector***

---

### **\$120 Million Spent on Storing and Retrieving Documents**

Mortgage financing is an important part of the economy—involving a wide range of financial institutions from commercial banks, thrifts and credit unions, finance companies, life insurers and government-sponsored enterprises like Fannie Mae. TowerGroup estimated that U.S. banks spent \$3.5 billion on mortgage compliance and processing technology in 2005, of which about \$120 million was spent on systems designed to store and retrieve documents used in closing and post-closing processes.

Over the years, Congress has enacted numerous laws to protect the consumer and prevent discrimination during and after the process of obtaining a mortgage loan. Complying with SOX, GLBA and many other mortgage regulations can be grueling and costly for lenders.



The ARC Morgan's financial consulting firm estimates that for every \$1 billion in annual sales, public companies spend \$2 million to \$3 million on systems upgrades, financial controls and consultants to comply with SOX alone. While mortgage company executives report increasing IT budgets for compliance purposes, some state they are also working to enhance the process for the customer and streamline the loan cycle for mortgage brokers.

### Home Mortgage Disclosure Act

The Home Mortgage Disclosure Act (HMDA) requires mortgage companies to maintain and report sensitive customer information. HMDA was enacted by Congress in 1975 and is implemented by the Federal Reserve Board's Regulation C. Today, this regulation applies to almost all institutions, including commercial banks, savings banks, credit unions and mortgage lending institutions and majority owned subsidiaries of depository institutions. HMDA requires them to maintain and annually disclose data about home purchases, home purchase pre-approvals, home improvement and refinance applications involving single and multifamily homes. The 1993 HMDA amendments require that all covered institutions must report the race or national origin, sex and income of the applicant or borrower.

Mortgage lenders are finding the regulatory demands cannot be met by strictly using traditional, paper-based processes, and many are converting to electronic processes to control procedures and increase efficiency.

Digitech Systems' ECM solutions provide the tools to comply with HMDA by offering the following capabilities:

- Capture software enables companies to convert paper documents to electronic files
- Automated importing and indexing improves productivity
- Powerful search capabilities allow companies to quickly and easily find information for annual disclosures
- Electronic distribution capabilities make sending information easy and cost effective
- Redaction hides sensitive information from unauthorized users and de-identifies information before disclosure
- On-demand access to information improves information accessibility and provides a comprehensive yet affordable solution

### Mortgage Sector: Moving to Electronic Processes

With an industry dependant upon complex approval processes and application reports, processing paper documents has become the single biggest operational headache for lenders. The sheer volume of paper makes storage an issue as well. Reclaiming paper storage space is a top priority, but so is speeding up the capture process once they decide to move to an electronic process. Keeping different types of forms in proper order and reducing human errors are also very important.

ECM is becoming an efficient and preferred method for managing loan documents and automating processes. Industry organizations such as Mortgage Industry Standards Maintenance Organization and the Mortgage Electronic Registration System are promoting new electronic data standards for mortgage lenders. Although participation is

*“With ECM, lenders can now move documents in sync with the data, share electronic documents online with multiple parties*



voluntary, the introduction of these new standards is driving companies to adopt automated, electronic processes.

The commercial and multifamily mortgage industry has started the migration to an e-commerce operating environment. According to the *2005 Mortgage Bankers Association Commercial Technology Survey*, more than three-quarters of survey participants have started efforts to store electronic images of loan documents. Nearly two-thirds of the loan proposals sent from originators to lenders were submitted electronically, and more than half of loan underwriting packages were received electronically. In addition, Investor reporting and remittances processes are all electronic.

Director of Consumer Lending at TowerGroup, Craig Focardi, told mortgage-technology.com, "With ECM, lenders can now move loan documents in sync with the data, share electronic documents online with multiple parties that need them and dramatically reduce their costs while speeding the sale of loans to the secondary market."

Using ECM, mortgage lenders can better manage a system that involves multiple parties, a vast amount of documents and various IT systems. Digitech Systems allows mortgage companies to:

- Capture, store and secure any information, document, email or file type
- Simplify information management with a single, searchable source
- Protect and control information and safely share documents
- Automate document routing to accelerate standard processes and improve customer service
- Monitor document history and user activity to ensure accountability and integrity
- Improve system accessibility with on-demand access, anywhere, anytime

## ***Digitech Systems' Solution***

---

The protection of information assets is necessary to maintain compliance with the law and protect the reputation of the institution. Timely and reliable information is essential to process transactions and support decisions. Digitech Systems solutions enable financial institutions to:

- Reduce costs associated with filing, managing, storing and retrieving information
- Improve efficiency with immediate information access and a programmed system that can route documents through approved or compliant processes
- Protect sensitive customer information, boosting customer confidence
- Control information access and security by defining user privileges
- Enhance security with electronic audit tracking that trace actions to their sources and prove technical and operational security measures are working
- Help institutions avoid fines and litigation associated with noncompliance

The table below matches regulations and requirements with PaperVision® Enterprise and ImageSilo® key features and benefits.

Financial Services Goal	Associated Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Protect personal and financial information	GLBA, HMDA, SOX, FDIC	<p>Multiple security levels</p> <p>Redaction</p> <p>Enhanced auditing</p>	<p>Control information access by user, project, document or specific index fields and restrict users' ability to view, change and share information</p> <p>Protect information by hiding it from users</p> <p>Force users to track disclosure methods, recipients and reasons</p> <p>Create a log for every document operation a user performs and track activity back to the user, assuring accountability and compliance</p>

Financial Services Goal	Associated Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Report information to customers and government agencies	GLBA, SOX, HMDA	PaperVision® Distribution Assistant  Document grants  Search capabilities including keyword searches  Enhanced auditing	Unlimited external media distribution saves printing and postage  Post documents to a secure, password protected, web-accessible location and disclose information only to authorized parties  Locate documents in seconds, search a single word or passage and pinpoint documents in seconds  Force users to track disclosure methods, recipients and reasons and ensure information was shared appropriately
Establish flexible and modifiable safeguards	GLBA	Changing system security policies	Flexible security controls, user access and system settings allow real time security adjustments

Financial Services Goal	Associated Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Pre-texting protection	GLBA	<p>ImageSilo system security</p> <p>ImageSilo data security</p> <p>Redaction</p> <p>256-bit AES encryption</p>	<p>Firewall technology protects against electronic intrusions</p> <p>Requested documents pass through firewall to a temporary cache directory</p> <p>Caching routines minimize the time information is on a public network</p> <p>Protect information by hiding it from users</p> <p>Encrypt data both during transmission and when stored to ensure information is protected</p>
Review customer communications and handle requests properly	NASD	<p>PaperVision Message Manager and PaperVision Enterprise WorkFlow</p> <p>PaperFlow and PaperVision Enterprise WorkFlow</p>	<p>Customer requests via email can initiate a workflow process to ensure proper procedures</p> <p>Scan written customer requests and initiate workflow processes to route documents accordingly</p>

Financial Services Goal	Associated Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Preserve key business records on a non-erasable media that is easily searchable	SEC Rule 17	PaperVision Enterprise  PaperFlow™  PaperVision® Distribution Assistant	Backup or store information to any media, including non-erasable media  Scan and index documents, then export them to any media for preservation  Distribute files to any external media and simplify document retrieval with self-contained retrieval capabilities
Produce easily readable images with enlargement capabilities	SEC Rule 17	QCFlow™ and PaperFlow	Quality control measures guarantee that processed text is accurately recognized with minimal operator intervention
Organize and index records accurately	SEC Rule 17	PaperFlow and QCFlow	Verify that captured data has been scanned properly and images are accurate  Image cleanup capabilities remove spots and repair misaligned documents to guarantee quality

Financial Services Goal	Associated Government Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Understand and document how significant transactions are initiated, authorized, supported, processed and reported to identify possible error sources	SOX	<p>PaperVision Enterprise WorkFlow and WorkFlow reports</p> <p>Enhanced auditing</p>	<p>Route documents through controlled procedural steps and produce reports showing how the process was executed</p> <p>Provide document history logs and user activity reports detailing who accessed a document when, what they did with it and why</p> <p>Audit reports provide tools for compliance and report user activity</p>
Establish and evaluate internal security controls for integrity and accountability	SOX, NASD Rule 3012, SEC Rule 17	<p>Multiple security levels</p> <p>Enhanced auditing</p>	<p>Control information access by user, project, document and/or specific index fields by limiting user activity</p> <p>Provide document history logs and user activity reports showing who accessed a document when, what they did with it and why</p> <p>Audit reports assure accountability and proof of compliance</p>

Financial Services Goal	Associated Government Regulation	PaperVision Enterprise/ ImageSilo Feature	Advantage/Benefit
Control user access to information and prevent unauthorized user activity	FDIC	<p>User-level, document-level, index field and project-level security</p> <p>Redaction</p> <p>Enhanced auditing</p>	<p>Control users' ability to read, share or change documents</p> <p>Control access by project, document and/or specific index fields</p> <p>Ensure users view only the information necessary for the task</p> <p>Protect information by hiding it from some users</p> <p>Force users to track disclosure methods, recipients and reasons</p> <p>Create a log for every operation a user performs and track activity back to the user</p> <p>Verify controls and identify unauthorized activity</p>
Deploy a disaster recovery plan	FDIC, SEC Rule 17	<p>ImageSilo</p> <p>Data Delivery</p> <p>Data Transfer Manager</p>	<p>Offsite data center offers internal and architectural redundancy, power redundancy and provides 24/7 monitoring</p> <p>Preserve identical copies of live information to any media on an automated schedule</p> <p>Package and encrypt information for delivery to any media on an automated schedule</p>

Monitor network traffic	FDIC	ImageSilo system security  Login security settings	Firewall technology controls network traffic and blocks unauthorized transmissions  Require all session activity to originate from the original login and restrict activity according to IP address(es)  If the IP address does not match, the system denies the request and sends a notification to system administrators
Password control features	FDIC	Password security settings	Control password expiration, strength, length and external account lockout  Limit opportunities for unauthorized access
Validate compliant methods with audits and other evidence	FDIC	Enhanced auditing        PaperVision Enterprise WorkFlow reports	Force users to track disclosure methods, recipients and reasons  Create a log for every operation a user performs  Provide document history logs showing who accessed a document when, what they did with it and why  Audit reports document system activity and can serve as a tool for compliance  Route documents through controlled steps and produce reports tracking progress
Control system settings and changes	FDIC	Global system administration or system administration	Global system administrators and/or system administrators can alter system settings and user security rights



In an industry where information and accurate recordkeeping is fundamental for success, PaperVision Enterprise and ImageSilo provide companies with the ability to have information at their fingertips, protect sensitive information, reduce human errors, improve customer service and deploy a disaster recovery strategy. Furthermore, these ECM systems help facilitate regulatory compliance for financial institutions and aid them in enhancing security and creating an information system that maintains integrity and accountability.

## ***Vocabulary and Terminology***

---

The following are some terms and concepts to be familiar with when speaking to a prospect in the financial services industry.

### **Federal Deposit Insurance Corporation (FDIC)**

Inspired by the Commonwealth of Massachusetts and its Deposit Insurance Fund (DIF), the FDIC is a United States government corporation created by the Glass-Steagall Act of 1933. The FDIC currently guarantees checking and savings deposits for member banks. Deposits are guaranteed up to \$100,000 per depositor.

### **Federal Financial Institutions Examination Council (FFIEC)**

The Federal Financial Institutions Examination Council is an interagency set out to dictate policies, standards and report forms for the scrutiny of financial institutions by the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, National Credit Union Administration, the Office of the Comptroller of Currency and the Office of Thrift Supervision.

### **Financial Industry Regulatory Authority (FINRA)**

On July 26, 2007, the U.S. Securities and Exchange Commission approved the formation of FINRA, a new securities self-regulatory body that succeeded the National Association of Securities Dealers (NASD) and consolidated it with the regulatory arm of the New York Stock Exchange. Although the organization has expanded, its mission remains the same—to regulate trading to ensure market integrity and investor confidence. See also NASD.

### **Firewall**

Firewalls are blocking mechanisms that control external network traffic both coming and going, in addition to a company's internal network traffic. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

### **Gramm-Leach Bliley Act (GLBA)**

Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLBA, includes provisions to protect consumers' personal financial information held by financial institutions. The GLBA gives authority to eight federal agencies and the states to administer and enforce regulations.

## Home Mortgage Disclosure Act (HMDA)

The Home Mortgage Disclosure Act (HMDA), enacted by Congress in 1975 and implemented by the Federal Reserve Board's Regulation C, requires lending institutions to report loan data.

## Mortgage Industry Standards Maintenance Organization, Inc.

Mortgage Industry Standards Maintenance Organization was established by the Mortgage Bankers Association to coordinate the development and maintenance of internet-based Extensible Markup Language (XML) real estate finance specifications. Their mission is to develop, promote, and maintain voluntary electronic commerce standards for the mortgage industry.

## National Association of Securities Dealers (NASD)

As the world's leading private-sector provider of financial regulatory services, NASD has helped bring integrity to the markets and confidence to investors. The NASD regulates trading in equities, corporate bonds, securities futures and options, with authority over the activities of more than 5,025 brokerage firms, approximately 169,470 branch offices, and more than 658,170 registered securities representatives. NASD members include virtually all investment banking houses and firms. Operating under the supervision of the SEC, the NASD's first purpose is to standardize practices in the field. See also Financial Industry Regulatory Authority (FINRA).

## Office of the Comptroller of the Currency (OCC)

The Office of the Comptroller of the Currency, a bureau of the U.S. Department of Treasury, was established by the National Currency Act of 1863 and serves to charter, regulate and supervise all national banks, federal branches and agencies of foreign banks in the United States.

## Pre-Texting

A collection of techniques used to manipulate people into performing actions or divulging confidential information. The term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim.

## Sarbanes-Oxley Act (SOX)

Overseen by the Securities and Exchange Commission (SEC), the Sarbanes-Oxley Act is a wide-ranging set of laws that established new or enhanced standards for all U.S. public company boards, management, and public accounting firms. These laws were the response to several major corporate accounting scandals. They cover financial audits and hold corporate officers responsible for the accuracy of financial statements. In particular, the act says that management must prevent—or detect in a timely manner—unauthorized acquisition, use, or disposition of systems that could affect financial data. It also specifies the kinds of records companies must keep and how long they must keep them.

## Serialize

The process of taking an object and converting it to a format that can be transported across a network or to a storage location. The storage location could be as simple as using a file or a database. The serialized format contains the object's state information.



Deserialization is the process of using the serialized state information to reconstruct the object from the serialized state to its original state. In essence, the process of serialization allows an object to be serialized, shipped across the network, stored in a location such as the ASP.NET cache and then be reconstructed for use at a later point in time.

### **U.S. Securities and Exchange Commission (SEC)**

The SEC is a federal agency created by the Securities Exchange Act of 1934 to administer that act and the Securities Act of 1933, formerly carried out by the Federal Trade Commission. The statutes administered by the SEC are designed to promote full public disclosure and protect the investing public against malpractice in the securities markets. The mission of the SEC is to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

## Case Studies

---

Testimonials and case studies showing how financial institutions are using Digitech Systems' software to comply with regulations and increase operational efficiency are available. Please see Digitech Systems' case studies at MyDSI.  
<http://mydsi.digitechsystems.com>



### **MacLean Financial Group**

MacLean Financial Group uses PaperVision Enterprise to trade expenses for revenue and increase clientele. With \$24,000 in annual savings, MFG funds new marketing efforts.



### **Randolph-Brooks Federal Credit Union**

With the installation of PaperVision Enterprise, bank employees reduce multiple transaction document retrieval from seven days to just minutes. They now capture and manage more than 25,000 documents every day, which greatly improves customer satisfaction and boosts employee morale.

# Digitech Systems

---

## ABOUT US

Digitech Systems, Inc. enables businesses of any size to more effectively and securely manage, retrieve and store corporate information of any kind. By significantly reducing the cost of Enterprise Content Management (ECM), Digitech Systems has moved ECM from a luxury to an essential element of a well-managed business.

Delivering the industry's smartest suite of ECM products and services, Digitech Systems is known by its customers as the trusted source for managing, storing and providing immediate, secure desktop or on-demand access to any and all corporate information. ImageSilo, PaperVision Enterprise, and a variety of document and content capture products are available as a fully integrated suite, or as process specific components to match the individual needs of small businesses to major corporations.

## CONTACT INFORMATION

Digitech Systems, Inc.  
8400 East Crescent Parkway, Suite 500  
Greenwood Village, CO 80111  
Toll Free: 866.374.3569  
Email: [sales@digitechsystems.com](mailto:sales@digitechsystems.com)  
[www.digitechsystems.com](http://www.digitechsystems.com)

© 2007 PaperVision, the PaperVision logo and ImageSilo are registered trademarks of Digitech Systems, Inc.

© 2007 PaperFlow is a trademark of Digitech Systems, Inc.