WHITE PAPER

The Critical Importance of Archiving in the Financial Services Industry

An Osterman Research White Paper

Published November 2011

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

OVERVIEW

The financial services sector is among the largest industries in the United States. For example, there are 6,413 FDIC-insured commercial banks and 1,100 savings institutions[i], 7,598 credit unions[ii], 4,525 members governed by the Financial Industry Regulatory Authority (FINRA)[iii], 631,085 FINRA-registered representatives[iv], more than 11,000 investment advisers registered with the Securities and Exchange Commission (SEC)[v], more than 275,000 state-registered investment adviser representatives[vi], and in excess of 15,000 state-registered investment advisers[vii]. Overall, the financial services industry in the United States employs approximately 5.8 million people and accounts for about six percent of total US GDP[viii].

While the sectors within the financial services industry are somewhat different from a regulatory standpoint, a common thread running across all organizations is the need to retain business records to varying degrees. For example, broker-dealers have the requirement to retain all communications – both those sent and those received – as well as written agreements related to their business activities; while banks, credit unions and advisers need to retain only certain types of content. The bottom line, however, is that every financial institution has an obligation to retain some of its records for long periods of time.

Because of the increasing proportion of content that is sent and received electronically in emails, other types of communications, and in other formats, financial services firms must deploy archiving systems that can a) index all relevant content, b) place this content into archival storage, and c) provide the ability to search for content on demand. A failure to implement appropriate archiving technology can result in significant financial penalties, as well as legal sanctions, loss of corporate reputation and other negative consequences.

THE FUTURE OF ARCHIVING IN FINANCIAL SERVICES

Some financial services firms do not archive their email and other electronic content because of their misperception that it is less expensive to pay the fines associated with non-compliance. That said, it is difficult to ascertain exactly how many firms fail to meet their retention obligations because few decision makers are willing to admit publicly that they are making a conscious decision to violate federal and other requirements for preservation of content. However, given the financial meltdown that began in late 2008, we can surmise with almost absolute certainty that government and industry oversight of the financial services sector in the context of data retention will become more stringent and more difficult over the next several years, and that archiving systems will play an even more important role in helping financial services firms to comply with their regulatory and legal obligations.

ABOUT THIS WHITE PAPER

This white paper discusses the requirement for financial services firms to retain content of various types, and it discusses what organizations should do to satisfy these obligations. It also provides a brief overview of ArcMail, the sponsor of this white paper and a leading provider of archiving systems.

Electronic Content Must Be Preserved

COMMUNICATION AND CONTENT MUST BE PRESERVED

More than virtually any another industry, the financial services industry has strict requirements to retain electronic content of all types. For example, securities dealers face the most stringent requirements:

- Since 1997, with the update of SEC regulations 17a-3 and 17a-4, regulated securities firms have had to retain email. Moreover, they must preserve this content on non-rewriteable media, provide a searchable index of the archived data, make it readily and quickly available when needed, and they must store a copy of their records at an offsite location for safekeeping.

- In July 2003, NASD rule 03-33 was issued that clarified regulated firms' requirements to retain instant messaging conversations.

- In January 2010, FINRA published Regulatory Notice 10-06 that clarified regulated firms' requirement to retain social media content.

The impact of the SEC and FINRA requirements is fairly straightforward: regulated firms must retain relevant content for long periods, and they must have ready access to this content when required, such as during a regulatory audit. The types of content that must be preserved include email, instant messaging and social media content with the public and with other employees; accounting records; memos; advertisements; stop orders; customer orders; correspondence; client complaints and other types of information that are in some way relevant to the trading operations of the firm and the regulated individuals.

Moreover, regulated firms must also supervise registered representatives through sampling or other means to ensure that they are in compliance with corporate and regulatory policies regarding the propriety of communications with customers and others.

In short, financial services firms must a) retain content and b) have the means to review it when required.

REQUIREMENTS VARY BASED ON ROLES AND FUNCTIONS

Requirements for the retention of data vary to some extent based on the role of the firms and the individuals offering financial services:

- **Broker-dealers**
  As discussed above, broker-dealer firms and their registered representatives face the most stringent requirements for content retention, including retention of records in a non-erasable format, serialization of the retained records, time/date stamping of the content, and the ability to download the indexes of the archived content, as well as the records themselves.

- **Hedge fund managers**
  Hedge fund managers also have specific requirements to retain email under SEC guidelines. Starting in February 2006, hedge fund managers/advisers with assets totaling more than

$25 million have had to register with the SEC in accordance with the Investment Advisers Act of 1940, making them liable for retention of email, instant messages and other relevant electronic content in much the same way that broker-dealers must preserve content.

- **Credit unions**
  Credit unions must also retain relevant records of various types in accordance with various requirements at both the Federal and state levels. For example, credit unions are required to comply with records retention requirements as set forth in 12 CFR, Part 749. The National Credit Union Administration's Rules and Regulations Part 749 recommends content retention requirements for credit unions, such as the maintenance of a geographically separate "Vital Records Center", although the NCUA does not regulate these practices.

  Examples of state requirements imposed on credit unions include:

  - Ohio's 1733.291 (Preservation of records – retention period – disposal) requires some records to be preserved for one year, while other records must be preserved for six years.

  - Hawaii's HRS 412:3-11(f) requires that no financial institution in the state "shall be required to preserve or keep its records or files for a period longer than six years, except as specified in subsection (g)".

  - Rhode Island Banking Regulation 98-5, Credit Unions, states, "Each credit union shall establish and maintain a written records retention and destruction program which shall be available to the Division of Banking at each examination for review and comment, but not approval. Such a program shall be in conformance with any applicable federal deposit insurance laws, rules, regulations or policies."

- **Banks**
  Banks must comply with a number of Federal and state requirements for retention of records. For example 12 CFR 27.5 requires that "Each bank shall retain the records required under 27.3 for 25 months after the bank notifies an applicant of action taken on an application, or after withdrawal of an application. This requirement also applies to records of home loans which are originated by the bank and subsequently sold." The Bank Secrecy Act of 1970 requires that banks retain records that might indicate money laundering, including cash purchases of negotiable instruments totaling more than $10,000 per day.

  Another Federal requirement, 12 USC 1829-Sec. 1829b (Retention of records by insured depository institutions) requires "the maintenance of appropriate types of records by insured depository institutions in the United States where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings…".

  There are also state requirements with which banks must comply, such as:

  - Vermont Regulation B-92-1 provides specific requirements for the retention of various types of banking records.

- Montana's 2.59.111 (Retention of Bank Records) sets forth minimum retention periods for various types of bank records.

- South Dakota's SDCL 51A-13-1 requires that "Every bank shall keep such books and accounts as the director may require for the purpose of showing the true condition of the bank, and shall keep accurate, convenient, and complete records of such transactions and accounts in permanent form."

THE BOTTOM LINE FOR ANY FINANCIAL INSTITUTION

Every financial institution – including very small ones – must comply with a growing number of records retention requirements imposed upon them at both the Federal and the state levels. We anticipate that these requirements will become more stringent and will be enforced more vigorously in the wake of the banking crisis that began in Fall 2008. The Restoring American Financial Stability Act of 2010 includes several records-related provisions, including Sec. 989(d), which states "For purposes of conducting the study required under subsection (b), the Comptroller General shall have access, upon request, to any information, data, schedules, books, accounts, financial records, reports, files, electronic communications, or other papers, things, or property belonging to or in use by a covered entity that engages in proprietary trading…". Moreover, a US government study published in January 2011[ix] discussed the potential for making investment advisers' content retention obligations more stringent.

The List of Requirements is Growing

THERE ARE MANY COMPLIANCE OBLIGATIONS

Financial services firms across the spectrum must satisfy a variety of regulatory obligations to preserve data, including:

- **SEC 17a-3 and 17a-4**
  Members of a national securities exchange, as well as their broker-dealers, must retain records that relate to their "business as such", including records of order entries, ledgers, account information, correspondence, puts[x], calls, spreads and other information that is relevant to their business. As noted earlier, hedge fund managers/advisers are now subject to Rule 17a-3 as a result of their requirement to register pursuant to SEC 203(b)(3)-2. SEC Rule 204-2 requires the books and records of investment advisers to be maintained, including journals, ledgers, written agreements and other business records.

  Rule 17a-4 specifies the length of time for preservation of records, as well as the manner in which these records are to be maintained.

- **FINRA Regulatory Notice 10-06**
  In January 2010, FINRA issued Regulatory Notice 10-06 that focuses specifically on social media content. The Notice focuses on financial services firms' use of blogs, social media sites, and other social networking tools. Among other things, the Notice delineates FINRA's requirement that firms are required to "retain records of communications related to the broker-dealer's business…made through social media sites", and "[regulated] firms must have a general policy prohibiting any associated person from engaging in business communications in a social media site that is not subject to the firm's supervision."

Moreover, recommendations of securities made through a social media site automatically trigger the requirements of NASD Rule 2310, a rule that governs firms' and registered representatives' recommendations about securities and other financial products.

- **NASD Rule 3010**
  This rule requires FINRA members to establish written procedures and a supervisory capability that will enable the organization to monitor the communications of its registered representatives. This normally involves sampling a percentage of emails in an archive to determine compliance with the written procedures.

- **NASD Rule 3110**
  This rule specifies that "Each member shall make and preserve books, accounts, records, memoranda, and correspondence in conformity with all applicable laws, rules, regulations, and statements of policy promulgated thereunder and with the Rules of this Association and as prescribed by SEC Rule 17a-3. The record keeping format, medium, and retention period shall comply with SEC Rule 17a-4."

- **Sarbanes-Oxley**
  The Sarbanes-Oxley Act of 2002 requires all public companies and their auditors to retain such relevant records as audit workpapers, memoranda, correspondence and electronic records – including email – for a period of seven years. Company officers are obliged to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses must ensure that employees preserve information – whether paper – or electronic-based -- that would be relevant to the company's financial reporting.

- **Gramm-Leach-Bliley Act**
  The Gramm-Leach-Bliley Act requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule (16 CFR Part 313) and the Safeguards Rule (16 CFR Part 314). The wide-ranging Safeguards Rule mandates what companies should include in their written information security plan and how to secure this information, including using tough-to-crack passwords and encrypting sensitive customer information when it is transmitted electronically via public networks. GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

- **Regulation S-P**
  Regulation S-P has been adopted by the SEC in accordance with Section 504 of the GLBA. This section requires the SEC and a variety of other US federal agencies to implement safeguards to protect non-public consumer information, and to define standards for financial services firms to follow in this regard. The rule applies to brokers, dealers, investment firms and investment advisers.

- **Payment Card Industry Data Security Standard**
  The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

  PCI DSS requirements impose a significant burden on any organization that generates electronic content. Sensitive and confidential data must be protected from interception by unauthorized parties, requiring the use of encryption and other safeguards.

- **Red Flag Rules**
  Part of the Safeguards Rule, the Red Flag Rules requires financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft. Affected businesses must develop and implement written identity theft prevention programs, which were required to be in place by Nov. 1, 2008. The programs "must provide for the identification, detection, and response to patterns, practices, or specific activities – known as 'red flags' – that could indicate identity theft."

While regulations like GLBA, Regulation S-P, PCI DSS or Red Flag Rules are ostensibly focused more on security issues, these requirements have important ramifications for archiving, as well, since archived content must be protected from unauthorized access or disclosure. Moreover, archiving technologies play a key role in helping organizations to satisfy PCI DSS and other requirements, since archived content can be the source data for an analytics system focused on identifying problems.

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

Financial services firms that do not comply with the various requirements for content preservation can face serious consequences, as shown in the following examples:

- In September 2011, Ayre Investments was censured and fined $10,000 for, among other things, permitting "its registered representatives to use email to conduct business when the firm did not have a system for email surveillance or archiving.[xi]"

- Also in September 2011, FINRA censured and fined E1 Asset Management $75,000 for a number of violations, including their failure to properly retain and archive instant messages sent or received by the firm's registered representatives[xii].

- In February 2011, FINRA reported that MBSC Securities, BNY Mellon Capital Markets and BNY Mellon Securities were censured and fined $300,000 for their failure to properly retain and review emails in a timely manner[xiii].

- In May 2010, FINRA fined Piper Jaffray $700,000 for failing to retain 4.3 million emails for a 73-month period ending in December 2008[xiv].

- In November 2009, FINRA fined MetLife Securities $1.2 million for their failure to supervise email communications adequately, a key requirement with which financial services are to comply in conjunction with their archiving obligations[xv].

- In February 2007, NASD fined four broker-dealers a total of $3.75 million for, among other things, not retaining the emails generated by 1,900 registered individuals[xvi].

- In February 2006, Morgan Stanley was fined $15 million for failing to retain emails[xvii].

- The firm Strand, Atkinson, Williams & York was $50,000 for, among other things, failing "to retain email messages in an accessible, reviewable format, and to review incoming and outgoing emails during a period of time.[xviii]"

- Brown Associates, a Tennessee-based broker-dealer, was fined $50,000 for, among other things, failing to properly archive some of its business-related emails[xix].

- A classic case of non-compliance was the December 2002 SEC settlement with five firms – Morgan Stanley, Salomon Smith Barney, Goldman Sachs, US Bancorp Piper Jaffray and Deutsche Bank Securities – for a fine of $1.65 million per firm for their failure to preserve electronic communications and their failure to establish, maintain and enforce a supervisory system[xx].

WHAT SHOULD ORGANIZATIONS DO TO REMAIN COMPLIANT?

It is important to note that while most of the SEC and FINRA fines have focused on larger institutions, smaller banks, credit unions, broker-dealers and others are just as vulnerable to fines and other sanctions for inadequate recordkeeping. Given that government oversight is increasing across all industries, but particularly in the financial services industry, every type of financial services organization must be vigilant to maintain adequate corporate governance practices and technologies in the context of records retention.

Another important caveat is not to fall into the trap of believing that paying fines is cheaper than establishing sound records retention policies and deploying good archiving technology. While in some rare cases that might have been true in the past, that is no longer the case. The tenor of government oversight is increasing and the fines will be increasing, making records retention and archiving significantly less expensive than paying the fines in virtually every case.

Steps to Address Compliance and Retention Obligations

Osterman Research recommends that organizations in the financial services industry – regardless of the aspect of the industry in which they participate – undertake a three-step approach to addressing their compliance and retention obligations:

- First, it's critical to understand that your organization must retain records that relate to a wide range of activities in your business. This is not an option for any company in the financial services industry, and so every company, regardless of its size, must develop policies focused on the retention of its business records. While many of the regulations that specify data retention are not necessarily clear about exactly what types of records to retain and which can safely be deleted, and while some may not be completely clear about the length of time that records should be retained, it is critical to retain relevant business records for long periods.
  The specifics of corporate policies will need to be hammered out in discussions with internal

and external counsel, compliance officers, regulators, consultants and others and will vary based on the particular products and services offered, the states in which a company operates, and so forth.

- Next, it is critical to deploy archiving technology that can satisfy content retention policies. Most organizations deploy systems that will archive emails and their attachments, but it may also be necessary to archive other types of content, such as files, social media posts, instant messaging conversations and other information. Keep in mind the potential need to sample employee email from the archive for compliance or monitoring purposes. Also focus on long-term data storage requirements and ensure that whatever archiving system you deploy will be able to satisfy long-term content retention goals in the context of storage space and speed of search across large data stores.

  It is important to note here something that may not be obvious to some decision makers: backups are not archives. While tape and/or disk backups of email and other servers is an important best practice, these backups are not a substitute for an archive.

- Finally, make sure that whatever archiving system you choose can integrate with and satisfy other requirements that your organization might have, such as making available content in a format that will satisfy regulators, external legal counsel and the like. The ability to provide content in a format that will enable easy transfer of information to others, particularly regulators, is essential because of the sometimes short windows that organizations are given to comply with orders to produce content.

Summary

Archiving in the financial services industry is absolutely essential – the option for decision makers' in the context of data retention is not whether or not to retain, but only how and how much to retain. Given that requirement and the likelihood that retention obligations will become more stringent in the future, it is vital that every financial services organization a) create retention policies and b) deploy the right archiving technology that will satisfy its long term goals.

About ArcMail

ArcMail is the e-mail archiving expert, solving critical business issues through best-in-class technology and services. Because all businesses need e-mail archiving, ArcMail provides enterprise-class solutions that are scalable to fit any sized business. ArcMail offers customers easy to use technology and provides the lowest total cost of ownership, optimizing their IT investment and providing immediate ROI.

ArcMail offers expertise in e-mail archiving issues such as legal eDiscovery, user and IT productivity improvement, network performance and storage capacity, and much more. ArcMail's Search and Retrieval capability is the fastest in the industry, in addition, tools and software are extremely easy to use, making it simple for clients to set up and start using within a matter of minutes.

[i] http://www.fdic.gov/bank/statistical/stats/2011jun/industry.html
[ii] http://www.pacreditunions.com/faqs.html
[iii] http://www.finra.org/Newsroom/Statistics/
[iv] http://www.finra.org/Newsroom/Statistics/
[v] http://www.sec.gov/news/studies/2011/913studyfinal.pdf
[vi] http://www.sec.gov/news/studies/2011/913studyfinal.pdf
[vii] http://www.sec.gov/news/studies/2011/913studyfinal.pdf
[viii] http://www.ita.doc.gov/td/finance/publications/U.S.%20Financial%20Services%20Industry.pdf
[ix] http://www.sec.gov/news/studies/2011/913studyfinal.pdf
[x] A "put" is an option contract giving the owner the right, but not the obligation, to sell a specified amount of an underlying asset at a set price within a specified time. Source: *Investopedia*
[xi] http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p124305.pdf
[xii] http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p124305.pdf
[xiii] http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p122925.pdf
[xiv] http://www.finra.org/newsroom/newsreleases/2010/p121506
[xv] http://www.finra.org/Newsroom/NewsReleases/2009/P120393
[xvi] http://www.finra.org/Newsroom/NewsReleases/2007/p018479
[xvii] http://www.computerworld.com/s/article/108687/Morgan_Stanley_offers_15M_fine_for_e_mail_violations
[xviii] http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p018298.pdf
[xix] http://complianceinsights.typepad.com/what_went_wrong/2011/08/tennesse-firm-censured-for-improperly-storing-emails.html
[xx] http://www.sec.gov/news/press/2002-173.htm