Technical Report

SEC 17a-4(f) Compliance Assessment

EMC Data Domain Retention Lock Compliance Software Product

Prepared by **Cohasset Associates, Inc.**

Abstract

This technical report is a compliance assessment of the EMC Data Domain Retention Lock Compliance software product capabilities relative to the requirements and conditions of SEC Rule 17a-4(f).

Cohasset's conclusion is that the EMC Data Domain Retention Lock Compliance software meets the relevant requirements of SEC 17a-4(f) in that during the SEC required retention period it: a) provides the integrated control codes and record file management capabilities that ensures protection of record files from overwrite or erasure; b) provides for initial and ongoing accuracy and quality of the stored records, c) uniquely identifies each record file and duplicate copy, and d) provides for a duplicate copy of the record files and recovery from the duplicate copy if required.

Cohasset Associates

7825 Washington Ave. South
Suite 500
Minneapolis, MN 55439-2415

www.cohasset.com

312-527-1550

1.1

CohassetAssociates

May 2013

Guiding the Way to Successful Records & Information Management

Table of Contents

1. Introduction

This section sets the context for this technical assessment. It identifies a) the SEC's regulatory foundation for allowing e-records to be retained on a variety of electronic storage media, and b) the storage system that is the subject of Cohasset's assessment against these SEC electronic storage media regulations.

1.1 The Electronic Storage Requirements of the Securities & Exchange Commission for 17a-4 Records

Records retention requirements for the U.S. securities broker-dealer industry are stipulated by the Securities & Exchange Commission ("SEC") Regulations 17 CFR 240.17a-3 and 17 CFR 240.17a-4 (the "Rule" or "Regulation"), adopted on February 12, 1997. Within this regulation, Rule 17a-4(f) expressly allows records to be retained on electronic storage media, subject to meeting certain conditions.

Three foundational documents collectively define and interpret the specific regulatory requirements that electronic storage systems must meet in order to be SEC compliant under Rule 17a-4(f).
They are:

- The Rule itself,
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4,* dated May 1, 2001 (the "2001 Release"), and
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records,* dated May 7, 2003 (the "2003 Release").

In the Rule and the two subsequent interpretative releases, the SEC clearly states that the use of electronic storage media and devices, to the extent that they can deliver the prescribed functionality, satisfy the stipulations of Rule 17a-4.

Rule 240.17a-4(f) specifically states:

> *The records required to be maintained and preserved pursuant to § 240.17a-3 and § 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form [emphasis added].*
>
> *(1) For purposes of this section:*
>
> * * * * *
>
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and f(1)(ii) of this section, which meets the applicable conditions set forth in this paragraph (f).*

The 2003 Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, may meet the requirements of a non-erasable, non-rewriteable recording environment – to the extent that they deliver the prescribed functionality and so long as appropriate integrated control codes are in place. The 2003 Release states:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*

The key words within this statement are "integrated" and "control codes." The term "integrated" means that the method used to achieve a non-rewriteable, non-erasable recording environment must be an integral part of the recording hardware and software. The term "control codes" indicates the acceptability of using attribute codes (metadata) that are integral to the hardware and software of the recording process in order to protect against overwriting or erasure of any records.

Examples of integrated control codes that could be applied towards providing a non-rewriteable, non-erasable recording process are:

- A retention period during which records cannot be erased,
- A unique record identifier that differentiates it from all other records, and
- The date/time of recording (the data/time of recording and the unique identifier serve in combination to "serialize" a record).

The 2003 Release specifically notes that recording processes or applications which merely mitigate the risk of overwrite or erasure (rather than prevent them), such as relying on access control security, will not satisfy the requirements of Rule 17a-4(f).

An important associated requirement of Rule 17a-4(f)(2)(i) is that a member, broker or dealer wanting to store their 17a-3 and 17a-4 records electronically must notify its "examining authority" ninety (90) days prior to employing any technology other than WORM optical media. Examining authorities are self-regulatory organizations (SROs) under the jurisdiction of the SEC such as the New York Stock Exchange (NYSE) and Financial Industry Regulatory Authority (FINRA).

1.2 Data Domain Retention Lock Compliance Software Product Overview

EMC offers a product named EMC Data Domain Retention Lock software which can be applied to any Data Domain Managed Tree (a logical volume in a virtual file system within a Data Domain deduplication storage system). When a Managed Tree is enabled to support Data Domain Retention Lock, a retention period can be set for individual record files that prevent the record file from being deleted before the retention period has expired. The Retention Lock capability can be configured with two types of software licenses: 1) a Data Domain Retention Lock Compliance software product license ("Retention Lock Compliance software product") that is designed to meet the requirements of SEC Rule 17a-4(f) and 2) a Data Domain Retention Lock Governance software product license where certain administrative functions may be performed that are not SEC compliant. This assessment report focuses solely on the Retention Lock Compliance software product license capabilties.

1.3 Assessment and Technical Report

To obtain an independent and objective assessment of the Retention Lock Compliance software product capabilities relative to meeting the requirements set forth in SEC Rule 17a-4(f), EMC engaged Cohasset Associates, Inc. ("Cohasset"), a highly respected consulting firm with specific knowledge, recognized expertise and more than 30 years of experience regarding the legal technical and operational issues associated with the records management practices of companies regulated by the SEC and SROs.

Cohasset's assignment was to:

- Assess the ability of the Retention Lock Compliance software product capabilities to meet the requirements of all the relevant conditions of Rule 17a-4(f), and
- Prepare this technical report regarding that assessment.

This assessment represents the professional opinion of Cohasset Associates and should not be construed as an endorsement or rejection by Cohasset of the Retention Lock Compliance software product and its capabilities or other EMC products. The information utilized by Cohasset to conduct this assessment consisted of: a) oral discussions, b) system requirements documents, c) user guides, and d) other directly related materials provided by EMC.

This assessment covers only the four requirements stated in SEC 17a-4(f) that relate directly to the recording, storage and retention management of regulated record files. The member, broker or dealer must ensure, however, that a combination of procedures, client application capabilities and the storage management capabilities addressed in this assessment meet all seventeen requirements of the Rule.

Additional information about Cohasset Associates is provided in Section 3 of this report.

The content and conclusions of this assessment are not intended and should not be construed as legal advice. Relevant laws and regulations are constantly evolving and legal advice must be tailored to the specific circumstances of the laws and regulations for each organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.

2. Compliance Assessment with SEC Rule 17a-4(f)

This section presents Cohasset's assessment of the EMC Data Domain Retention Lock Compliance software product capabilities that are relevant to meeting the electronic records storage requirements of SEC Rule 17a-4(f).

2.1 Structure and Organization of Cohasset's Assessment

The assessment of each relevant requirement in Rule 17a-4(f) is structured into four parts:

Compliance Requirement – Definition of the specific SEC regulatory requirements that must be met in order to utilize electronic records storage media in the retention of 17a-3 and 17a-4 records;

Compliance Assessment – Cohasset's assessment of the degree to which Retention Lock Compliance software product capabilities comply with the Rule;

Retention Lock Compliance Software Product Capabilities – Description of the Retention Lock Compliance software product capabilities that enable them to meet the specific 17a-4(f) requirement; and

Other Considerations – Identification of actions (if any exist) that may need to be performed in order to meet the requirements of the Rule.

Note: The term "record" is utilized in SEC Rules 17a-3 and 17a-4 to describe all information content that must be retained under the Rules. Since this assessment deals with the capabilities of the Retention Lock Compliance software product relative to SEC Rules, Cohasset Associates has chosen to use the term "record" or "record file" (versus "file") in order to be consistent with SEC terminology.

2.2 Non-rewriteable, Non-erasable Format

2.2.1 Compliance Requirement 17a4(f)(2)(ii)(A)

Preserve the records exclusively in a non-rewriteable, non-erasable format.

As set forth in Section III (B) of the 2001 Release, this requirement "is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in unalterable form."

The following statement in the 2003 Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, would meet the requirements of a non-erasable, non-rewriteable recording environment provided a) they deliver the prescribed functionality and b) that functionality is delivered via appropriate integrated control codes for the SEC designated retention schedule associated with the stored record:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*

2.2.2 Compliance Assessment

It is Cohasset Associates' opinion that the Retention Lock Compliance software product provides very strong capabilities for meeting this requirement of the Rule, provided certain capabilities discussed below are properly configured and applied by the member, broker or dealer and that any conditions stated in subsection 2.2.4, "Other Considerations" are met.

2.2.3 Retention Lock Compliance Software Product Capabilities

The main features of the Retention Lock Compliance software product that support meeting the non-rewritable and non-erasable requirement of the Rule are:

- The member, broker or dealer must purchase unique Retention Lock Compliance software product licenses, as required, which ensure that the "compliance" features of Retention Lock are activated.
- During administrative setup of the Retention Lock Compliance software product, one or more Managed Trees can be defined as being under Compliance control, thereby allowing retention management to be applied to recorded files.

- After a Managed Tree has been configured with Retention Lock Compliance software product it cannot be disabled, overridden or deleted.
- For a Managed Tree (MTree) that is Retention Lock Compliance software enabled, a record file can be placed under retention management control by setting a time-based[1] retention period (in the form of a retention expiration date). The retention period is set when the client application, e.g., an e-mail archiving application or file archiving application a) issues a file protocol instruction with an "atime"[2] attribute retention value that is set into the future (beyond current date/time) and b) where the retention period is greater than the Minimum defined retention period per MTree and less than the Maximum defined retention period per MTree.
- The initial retention period value and any valid retention period extension value thereafter is extracted from the atime attribute and stored as a protected file directory entry that is retained for the same period of time as the associated record file.
- A Minimum and Maximum retention period for each MTree must be established during the administrative setup of the Retention Lock Compliance software on EMC Data Domain systems. This ensures that the initial retention period for a record file and any subsequent retention period extension is not set below the Minimum or above the Maximum. Once set, the Minimum and Maximum retention periods can only be extended (such as increasing the Maximum to accommodate a legal hold) but they cannot be reduced.
- The retention period is then managed as follows:
    - Any retention period atime value that is less than or equal to current time – and therefore not a valid retention period – is ignored since it is assumed to be an update to the "time last accessed" value.
    - Any retention period value that is less than the Minimum retention period or greater than the Maximum retention period per Managed Tree will result in an error condition being returned to the client application.
    - The retention period for any record file may be extended by recording a new atime retention value for a record file that is later in time than the current retention period but not later in time than the Maximum retention period.
    - If an attempt is made to delete a record file before the retention period has expired, the delete command is rejected and results in an error condition.

  - If an attempt is made to delete an MTree that is Retention Lock Compliance software enabled and currently contains record files, then the delete command is rejected and results in an error condition.
  - Once the retention period has expired, deletion of the record file may be performed by an authorized client application or administrator.
- A Compliance Managed Tree cannot be deleted under any circumstances.
- When a Retention Lock Compliance software product license is un-installed, has expired or is cancelled for any reason, no new Compliance Managed Trees can be defined. However, all of the record files in all existing Compliance Managed Trees will continue to be protected in accordance with the SEC Rule. Also any new files that are stored in existing Compliance Managed Trees with a retention period later than the date stored will be protected in a manner compliant with the SEC Rule.
- Additional administrative security is provided in the Retention Lock Compliance software product to ensure that certain administrative functions or actions that could potentially compromise the integrity of record files prior to expiration of the retention period are not under the control of just one administrative person. This additional administrative security is provided in the form of a dual sign-on, i.e., sign-on by the regular system administrator plus the requirement for second sign-on by an authorized person. Data Domain refers to this feature as the "Security Officer" sign-on (see 2.2.4 Other Considerations). The primary administrative actions that require a dual or Security Officer sign-on in a Retention Lock Compliance software product are:
  - Extending Minimum or Maximum retention periods.
  - Renaming an Managed Tree.
  - Deleting a Retention Lock Compliance software product license.
  - Other system support or maintenance actions that could potentially compromise the integrity of stored record files where the retention period has not expired.
- The accuracy of the system clock in a Retention Lock Compliance software product is critical for determining whether the retention expiration date of a record file has expired. Situations can occur, such as a power outage, maintenance downtime, etc., which may affect the accuracy of the system clock and require it to be adjusted or reset. Additional statistics are gathered, analyses are performed and certain restrictions are placed on ensuring the accuracy of the system clock to meet retention compliance requirements.

    - The accuracy of the system clock and variations of the system clock with current actual time is regularly monitored.
    - The system clock is only allowed to vary by a maximum of two weeks in a year.
    - Should the system clock vary beyond the two week maximum during a year, then the administrative Security Officer dual sign-on is required to reset the clock to current time.

- No logical access (via a software user interface) without Security Officer dual sign-on is allowed for error correction purposes such as the scenario where the Retention Lock Compliance software product experiences a system error or corruption. For the extreme scenario where the full Data Domain operating system will not start up, a restart of the operating system is restricted to single user access via the use of a USB drive which must be physically protected and made accessible only with a second authorization by a Compliance Officer or Security Officer.
- An Managed Tree that is configured as Retention Lock Compliance software product can store files that are not regulated as records under the Rule and, as such, do not require a retention period to be set. Therefore, record files required to be compliant with the Rule as well as non-regulated files can be intermixed on the same Retention Lock Compliance software product Managed Tree (see *2.2.4 Other Considerations*).

2.2.4 Other Considerations

The following actions should be undertaken to ensure that the compliance features of the Retention Lock Compliance software product are activated and configured to meet the requirements of the Rule:

- The member, broker or dealer must purchase a unique Retention Lock Compliance software product license which ensures that the features of the Retention Lock Compliance software product necessary to meet the requirements of the Rule are applied.
- Where administrative functions require a dual or second sign-on (Security Officer sign-on), Cohasset Associates strongly recommends that the authorized second sign-on person be the equivalent of either a Chief Compliance Officer or a Chief Security Officer or their representative as designated in writing.
- It is imperative that the member, broker or dealer insure that the client application which is writing record files regulated under the Rule sends the appropriate retention period for each record file to the Retention Lock Compliance software product.

2.3 Verify Automatically the Quality and Accuracy of the Recording Process

2.3.1 Compliance Requirement 17a-4(f)(2)(ii)(B)

Verify automatically the quality and accuracy of the storage media recording process.

The intent of SEC Rule 17a-4(f)(2)(ii)(B) is to ensure that the media recording process is accurate to a very high degree and, therefore, the recorded information is of the highest quality. The objective of this subsection of the SEC Rule is to provide the utmost confidence that all records read from the storage media are precisely the same as those recorded.

2.3.2 Compliance Assessment

Cohasset believes that the Retention Lock Compliance software product provides exceptional capabilities for meeting the SEC requirement to verify the accuracy and completeness of the recording process.

2.3.3 Retention Lock Compliance Software Product Capabilities

The Retention Lock Compliance software product employs a comprehensive Data Invulnerability Architecture for enhanced data integrity and recoverability. The Data Invulnerability Architecture provides for end-to-end verification using the following capabilities: immediate read back and verification at the time of recording, fault avoidance and containment, continuous fault detection and correction, and file system and Managed Tree recoverability. The capabilities of the Retention Lock Compliance software product that directly support the verification of the quality and accuracy of the recording process are:

Initial Recording Process

- The Retention Lock Compliance software product provides an exceptionally strong capability for verifying quality and accuracy in that for each container of record file data that is written, an immediate read back is performed and the accuracy of the recording is verified before being accepted as error-free. This method goes beyond the minimum acceptable reliance on state-of-the-art magnetic disk recording error checking and detection/correction capabilities.

Post Recording Process

- Record file data is packaged and written in containers (multi megabyte units). A strong checksum value is calculated from the data in each container and stored with that container. The write verification process involves reading back the data in the stored containers and verifying that the checksums are accurate. After the containers are verified, the files contained in them are verified by reading the metadata of the files and verifying that each segment of a file exists in the containers identified by the metadata.
- During read back of a record file, whether by the client archiving application or by the Data Domain file system, the checksums are verified and, when errors are encountered, RAID 6 error correction is applied as required thereby ensuring that the record remains complete and accurate.
- During verification, if the container cannot be recovered using RAID 6, an alert is raised to the client application whereupon the administrative support personnel can recover the data from a replicated or duplicate copy.
- Periodic "scrubbing" of the record file data on the Retention Lock Compliance software product is performed to find and correct any defects that may occur. This is particularly important for those record files that have not been read back for an extended period of time.

2.3.4 Other Considerations

There are no other considerations related to this requirement.

2.4 Serialize the Original and Duplicate Units of Storage Media

2.4.1 Compliance Requirement 17a-4(f)(2)(ii)(C)

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.

This requirement, according to Section III(B) of the 2001 Release, "is intended to ensure both the accuracy and accessibility of the records by indicating the order in which records are stored, thereby making specific records easier to locate and authenticating the storage process."

While this requirement is thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage, the SEC Rule may be satisfied for electronic records by capturing index or metadata associated with each record file that: a) "uniquely" identifies the record file, and b) associates a "date of recording" with each record file.

2.4.2 Compliance Assessment

Cohasset believes that Retention Lock Compliance software product meets the SEC requirement to serialize both the original record and each duplicate copy stored.

2.4.3 Retention Lock Compliance Software Product Capabilities

The following capabilities of the Retention Lock Compliance software product are designed to meet the requirement of the Rule.

- The Retention Lock Compliance software product identifies each record file with a unique user ID which contains a unique file name and date/time recorded stamp, thereby uniquely identifying each record file logically and chronologically.
- When record files managed under the Retention Lock Compliance software product are replicated to another Data Domain system with the Retention Lock Compliance software product, the unique file name and data/time stamp as well as all retention metadata attributes are duplicated.

2.4.4 Other Considerations

There are no other considerations related to this requirement.

2.5 Store Separately a Duplicate Copy

Compliance Requirement 17a-4(f)(3)(iii)

Store separately from the original a duplicate copy of the record stored on any medium acceptable under 240.17a-4 for the time required.

The intent of this requirement is to provide an alternate storage source for accessing the record should the primary source be compromised, i.e., lost or damaged.

Note: A "duplicate copy" is different from a backup copy in the sense that the duplicate copy is the recording of a real-time copy of the record or recording a one-for-one "journal" copy of the record that is never overwritten or erased. Backup copies, on the other hand, may be overwritten as they are "rotated" on a periodic basis.

2.5.2 Compliance Assessment

It is Cohasset's opinion that Retention Lock Compliance software product complies with this SEC requirement.

2.5.3 Retention Lock Compliance Software Product Capabilities

- The Retention Lock Compliance software product provides for an Managed Tree to be replicated to a second Retention Lock Compliance software product Managed Tree, either locally or remotely. During Replication, all record file data and associated metadata, including retention metadata, are replicated to the second file system or Managed Tree.
- Should a major error occur that makes the original file system or Managed Tree inaccessible, then the record files can be recovered from the replicated copy of the Managed Tree.

2.5.4 Other Considerations

There are no other considerations related to this requirement.

3. Conclusions

This technical assessment has addressed whether the Retention Lock Compliance Storage System capabilities meet the requirements and conditions of SEC Rule 17a-4(f).

Cohasset's opinion is that the Retention Lock Compliance Storage System:

- Meets the requirements of the Rule for preserving the records in a non-erasable, non-rewriteable format through the use of integrated control codes and records retention management functionality.
- Meets the requirements of the Rule related to the automatic verification of the accuracy and quality of the recording process in that it employs a comprehensive Data Invulnerability Architecture that immediately reads back and verifies each container of record file data stored, and utilizes state-of-the-art error detection and RAID 6 technology to correct any errors detected during read-back and periodic scrubbing.
- Uniquely identifies and serializes each record and duplicate copy that is stored.
- Supports storing a compliant duplicate copy of each record and provides for the recovery of record files from the duplicate copy.

Cohasset Associates' conclusion: The Retention Lock Compliance Storage System meets all of the SEC requirements that are its direct responsibility for retaining and storing in digital form 17a-3 and 17a-4 records – pursuant to all the requirements set forth in Rule 17a-4(f), which expressly allows records to be retained on electronic storage media.

End Notes

1. Retention Lock currently supports only time-based retention (i.e., retained for a specified period from the time after the file is recorded). Event-based retention (i.e., indefinite retention once the file is recorded until a specified event occurs, followed by a fixed, final retention period) is not currently supported.

2. The "atime" attribute in standard file protocol instructions represents the "time last accessed" for a file. For Retention Lock Compliance software enabled Managed Trees, this attribute is utilized to establish the retention expiration date for a record file.

3. Redundant Array of Independent Disks (RAID): A method for recording data to magnetic disk devices that provides for various levels of error correction and read or write performance improvements. RAID 6 employs striped disks with dual parity and combines four or more disks in a way that provides for correction of detected errors for up to as many as two full disk units of data during read back.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com), is one of the nation's foremost consulting firms specializing in records and information management. Now in its fourth decade of serving clients throughout the United States, Cohasset Associates provides award-winning professional services in three areas: management consulting, education and legal research.

Management Consulting: The focus of Cohasset Associates' consulting practice is improving the programs, processes and systems that manage document-based information. Cohasset works to provide its clients with cost-effective solutions that will both achieve their business objectives and meet their legal/regulatory responsibilities. This ranges from establishing effective corporate records management programs to planning state-of-the-art electronic records systems.

Education: Cohasset Associates is renowned for its longstanding leadership in records management education. Today, Cohasset's educational work is centered on its annual National Conference for Managing Electronic Records (MER), which addresses the operational, technical and legal issues associated with managing the complete life cycle of electronic records (www.merconference.com). The MER sessions also are available at RIM on Demand.
(www.rimeducation.com/videos/rimondemand.php)

Legal Research: Cohasset Associates is nationally respected for its leadership on records management legal issues – from retention schedules to the use of alternative media to paper for storing document-based information.

For more than twenty years, Cohasset Associates has been a "thought leader" in records and information management. Cohasset has been described as the only management consulting firm in its field with its feet in the trenches and its eye on the horizon. It is this blend of practical experience and a clear vision of the future that, combined with Cohasset Associates' commitment to excellence, has resulted in Cohasset Associates' extraordinary record of accomplishments and innovation.