SEC 17a-4(f) & CFTC 1.31(b)-(c) Compliance Assessment

Amazon Glacier with Vault Lock

Prepared by: **Cohasset Associates Inc.**

Abstract

Amazon Glacier ("Glacier") is a very large-scale, cloud-based archival storage service optimized for infrequently accessed data, or "cold data." When properly configured and when Vault Lock policy capabilities are correctly applied, Glacier provides integrated control codes and other relevant capabilities that prevent stored Archive records from being overwritten, deleted or altered until the specified retention period has expired.

In this Assessment Report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Glacier responsive to the storage requirements of the:

- Securities and Exchange Commission (SEC) in regulation 17 C.F.R. § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Commodity Futures Trading Commission (CFTC) in regulation 17 C.F.R. § 1.31(b)-(c), which regulates commodity futures trading.

It is Cohasset's opinion that Glacier, when properly configured and utilized in conjunction with Vault Lock to store and retain records in non-erasable and non-rewriteable format, meets the relevant storage requirements of SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c).

See Section 2 for the details of Cohasset's assessment, Section 3 for a summary of Cohasset's conclusions, and Section 4 for an overview of the relevant SEC and CFTC Rules.

CohassetAssociates

August 2015

7825 Washington Ave. S., #500 | Minneapolis, MN 55439-2415 | USA | 312.527.1550 | **www.cohasset.com**

Table of Contents

1. Introduction

The Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) define rigorous and explicit requirements for organizations that elect to retain books and records on electronic storage media.

Given the prevalence of electronic retention of books and records, these requirements apply to most broker-dealer and commodity future trading firms and other support organizations with regulated functions or operations.

Amazon added the Vault Lock capabilities to the Glacier archival storage system in order to meet the stringent SEC and CFTC electronic records requirements for the receipt, storage and retention of regulated books and records. To evaluate its compliance with the SEC and CFTC requirements, Amazon engaged Cohasset to complete an independent and objective assessment of the Glacier archival storage system and the Vault Lock capabilities relative to meeting these requirements.

This Introduction *briefly summarizes the regulatory environment, explains the purpose and approach for Cohasset's assessment, and provides an overview of the Glacier archival storage system and Vault Lock.*

1.1 Overview of the Regulatory Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4, the SEC stipulates recordkeeping requirements, including retention periods, for the securities broker-dealer industry. On February 12, 1997, the SEC adopted revisions to 17 CFR § 240.17a-4 (the "Rule" or "SEC Rule 17a-4"). These revisions to paragraph (f) expressly allowed books and records[1] to be retained on electronic storage media, subject to explicit conditions. Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f). This Assessment Report includes a summary of the Rule and these two Interpretive Releases in Section 4.1, *Overview of SEC Rule 17a-4(f) Electronic Storage Requirements*.

Additionally, the Financial Industry Regulatory Authority (FINRA) Rule 4511(c) definitively defers to the format and media requirements of SEC Rule 17a-4, for the books and records that it requires.

In 17 CFR § 1.31 ("CFTC Rule 1.31"), the CFTC defines rigorous requirements for organizations electing to retain books and records on electronic storage media. The June 28, 1999 revisions were the first to authorize

[1] Regulators use the phrase "*books and records*" to describe all content that must be retained under the Rules. Since this assessment deals with the capabilities of a storage solution relative to SEC Rules, Cohasset has chosen to use the term "record" (versus "data" or "file") to be consistent with SEC terminology.

books and records to be retained on electronic storage media, subject to explicit conditions. This Assessment Report includes a summary of these requirements in Section 4.2, *Overview of CFTC Rule 1.31(b)-(c) Electronic Storage Requirements*.

Additionally, for the comparable requirements of SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), see Section 4.3, *Comparison of Relevant Requirements of SEC and CFTC Rules*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the capabilities of the Glacier archival storage system and Vault Lock functionality, in comparison to the requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), Amazon engaged Cohasset Associates, Inc. ("Cohasset"). Cohasset is a highly respected consulting firm with more than 40 years of experience and knowledge related to the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and the CFTC. Additional information about Cohasset is provided in the last section of this report.

Cohasset was engaged to:

- Assess the Glacier archival storage system, in conjunction with Vault Lock capabilities, in comparison to the five requirements related to the recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), and
- Prepare this Assessment Report enumerating the results of its assessment.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection by Cohasset of the Glacier solution and its capabilities or other Amazon products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) user and system administration documentation, and (c) other directly-related materials provided by Amazon or gleaned from publicly available sources.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented solutions, meet all seventeen requirements of the Rule.

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

1.3 Amazon Glacier and Vault Lock Overview

Glacier is a very large-scale, cloud-based archival storage service optimized for infrequently accessed data, or "cold data." Data is stored under an "Account" name in containers called "Vaults". Each individual file uploaded to a Glacier Vault is called an "Archive." Each Account can have up to 1,000 Vaults and each

Vault can store an unlimited number of Archives. An Archive can be any set of data such as a photo, video, report or any document format.

Either a single file or multiple files aggregated into a compressed file (such as a TAR or ZIP file), may be uploaded as one Archive. Each Archive is assigned a unique Archive ID at the time of receipt and is stored separately from all other Archives. Glacier is inherently a "write-once" storage system – the content of a stored Archive is controlled such that it cannot be overwritten, updated or altered. Within a Vault, policies are established to grant or deny specific activities, such as user access and deletion rights.

Amazon added the Vault Lock policy capabilities to Glacier with the objective of meeting the more stringent retention and preservation requirements of SEC Rule 17a-4(f) and other similarly rigorous regulatory requirements. The Vault Lock policy incorporates integrated controls – such as a retention period, a lockdown feature that prevents premature Archive deletion, and the use of legal hold settings – to provide immutable retention management and deletion protection of Archive records, as well as setting and releasing legal holds at the Vault level.

This Assessment Report focuses on the relevant capabilities of the Glacier archival storage system functionality and the Vault Lock capabilities that are designed to meet the SEC requirements.

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

This section presents Cohasset's assessment of the capabilities of the Glacier archival storage system, in conjunction with Vault Lock, for compliance with the five requirements related to the recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f). See Section 4.3, Comparison of Relevant Requirements of SEC and CFTC Rules.

For each of the five relevant requirements in SEC Rule 17a-4(f), this assessment is organized into the following four topics:

Compliance Requirement – A brief explanation, prepared by Cohasset, of the purpose of the specific requirement of the Rule;

Compliance Assessment – Preliminary assessment of the Glacier and Vault Lock capabilities in relation to compliance with the specific requirement of the Rule,

Capabilities of Amazon Glacier with Vault Lock – Description of the Glacier capabilities necessary to meet the requirement; and

Considerations – Considerations for meeting the specific requirement.

The following subsections document Cohasset's assessment of the capabilities of the Glacier archival storage system with Vault Lock relative to each pertinent requirement of the Rule.

2.1 Non-Rewriteable, Non-Erasable Record Format

2.1.1 Compliance Requirement SEC 17a-4(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 Interpretive Release, this requirement *"is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in an unalterable form."*

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-erasable and non-rewriteable recording environment provided: (a) the storage solution delivers the prescribed functionality, and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

> *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.*

Further, Section IV of the 2003 Release places requirements on the storage system for retaining records beyond the SEC-established retention period when certain circumstances occur, such as a subpoena or hold order:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules. [emphasis added]*

This statement by the SEC clarifies that the storage system must have the capability to retain records beyond the retention period established at the time of initial recording when required for legal matters, external investigations or audits, or other similar circumstances.

2.1.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Glacier with Vault Lock meet the requirements of the Rule for (a) managing the retention of *time-based*[2] records as non-rewritable and non-erasable and (b) preserving records pursuant to a legal hold, when the considerations identified in Section 2.1.4 are satisfied.

2.1.3 Capabilities of Amazon Glacier with Vault Lock

In this section, the capabilities of Glacier and the Vault Lock functionality that affect meeting the requirements of SEC Rule 17a-4(f) for preserving broker-dealer electronic records[3] as non-rewritable and non-erasable, are presented.

- Glacier stores record files within a hierarchy of: (a) Account, (b) Vault, and (c) Archive. At least one Account must be configured. Within each Account, a minimum of one and a maximum of 1,000 Vaults may be configured. Each Vault can store an unlimited number of Archives.
- The term "Archive" is used to designate files that are uploaded to, and stored in, Glacier. Each Archive may be comprised of either a single file or an aggregation of multiple files into a compressed file type, such as a TAR or ZIP file.

[2] Time-based retention periods use the creation or storage date to calculate the retention expiration date. As noted in Section 2.1.4, conditional or event-based retention periods, which use a triggering date, are not supported by Glacier.

[3] The term "Archive" or "Archive record," rather than just "file" or "Archive file," is used in this document to reflect the fact that business transactions, customer information, broker-dealer personnel and certain other administrative files are deemed *business records* that are required to be maintained for a specific period of time (the retention period) as stated in SEC Rules 17a-3 and 17a-4.

- Glacier stores each uploaded Archive as a completely separate object that cannot be overwritten, updated or altered. Accordingly, Glacier is a non-overwrite object storage system.
- Archive records are uploaded to a Vault by a client application using the appropriate Glacier application programming interface (API). During the upload process, Glacier generates a unique Archive ID. Once the Archive has been successfully uploaded and stored, Glacier sends the unique Archive ID to the client application to be used for retrievals and downloads.
- One of each of the following two types of policies can be applied to a Vault:
  - *Vault Lock policy:* A Vault-level policy, which must be locked down to provide immutable controls for managing retention and deletion protection. A locked Vault Lock policy establishes a minimum time-based retention period and prevents attempts to delete the Archive records prior to the expiration of the minimum retention period.
  - *Vault access policy:* A modifiable Vault-level policy that may be utilized to (a) establish retrieval privileges, (b) grant temporary third-party access privileges, (c) specify a Vault retention period, and (d) control other Vault-level actions.
- For each Vault Lock policy, two steps must be taken to make the policy immutable.
  - **Step 1:** The client application must issue an "InitiateVaultLock" API call to Glacier specifying the Vault to be locked and providing an "ArchiveAgeInDays" retention period for the Vault.
    - This step sets the Vault Lock policy to an *in-progress* state, which:
      - Effectuates the ArchiveAgeInDays retention control.
      - Allows the broker-dealer to test the ArchiveAgeInDays retention period and other controls or tags associated with the policy.
      - Issues a "Lock ID" and returns it to the client application. This Lock ID must be specified in the CompleteVaultLock call (see below) to fully lock the designated Vault.
    - An in-progress Vault Lock policy can be deleted using an AbortVaultLock API call from the client application, should the policy controls require adjustment.
    - An in-progress Vault Lock policy automatically expires after 24 hours and is disassociated from the Vault. A new InitiateVaultLock call must be made to the Vault to reinitiate the in-progress state of the Vault and provide a new Lock ID to the client application.
  - **Step 2:** The client application must issue a CompleteVaultLock API call with the Vault name and the Lock ID (issued with the InitiateVaultLock call), which makes the Vault Lock

    policy controls, including the ArchiveAgeInDays, immutable. Once the policy is locked down:

    - The ArchiveAgeInDays retention period of the Vault, in conjunction with the upload date of each Archive, is used to calculate the retention expiration date.
    - The Archive is protected from deletion until the retention expiration date for the Archive is met. (See Vault access policy below.)

- Only one Vault Lock policy, and associated ArchiveAgeInDays retention period, can be assigned to a Vault. Therefore, a sufficient number of Vaults must be defined, with appropriate Vault Lock policies, to accommodate each time-based retention period for the Archives to be stored in the Account.
- Once the Vault Lock policy, with an ArchiveAgeInDays, has been locked, the following controls apply:
    - Archive records stored in the Vault cannot be deleted, overwritten or modified – from any source or by any command – until the retention period has expired.
    - Only one Vault Lock policy can be assigned to a Vault. Any attempt to assign a second Vault Lock policy to a Vault will be denied.
    - The Vault Lock policy cannot be deleted from the Vault.
    - The Vault can only be deleted when the retention period for all Archives in the Vault have expired and have been deleted from the Vault, i.e., when the Vault is empty.
    - When a delete command for a specific Archive is issued, via a client application API, the retention expiration date is calculated by adding the Vault Lock policy ArchiveAgeInDays retention period to the upload date of the Archive to be deleted. If the expiration date has not been reached, then the deletion command is denied.
    - The ArchiveAgeInDays can be extended, but not shortened, using the Vault access policy, as noted below.
- In addition to the Vault Lock policy, one Vault access policy can be assigned to a Vault. The Vault access policy provides flexible controls that can be modified or deleted by authorized personnel. The Vault access policy can be used to define retrieval privileges, to grant temporary third party access rights and to establish an ArchiveAgeInDays retention period, among other controls. When the Vault access policy establishes an ArchiveAgeInDays retention period:
    - The Vault will retain Archive records for the longest ArchiveAgeInDays retention period that is assigned to the Vault by either the Vault Lock or Vault access policies.
    - If the Vault access policy is deleted or the ArchiveAgeInDays retention period of the Vault access policy is changed to a period shorter than that of the Vault Lock policy, then the retention period control defaults to the ArchiveAgeInDays retention period specified in the Vault Lock policy.

- When a subpoena or legal hold requires one or more Archive records to be preserved, a legal hold tag ("LegalHold: "true" or "false") can be assigned to the entire Vault, via the API.
    - The legal hold tag prevents deletion of Archives until the tag is removed. Once removed, the ArchiveAgeInDays retention periods associated with the Vault govern retention and deletion eligibility.
    - A Vault with a legal hold tag cannot be deleted until the legal hold tag is removed.
- Another method of supporting legal hold is to assign a Vault access policy with an ArchiveAgeInDays that is equivalent with the anticipated term of the legal hold.
    - When the legal hold has expired, the Vault access policy can be deleted or the ArchiveAgeInDays retention period of the policy can be removed or shortened.
    - If the legal hold is extended, the ArchiveAgeInDays must be lengthened to cover the entire period of the legal hold.
- For an Archive deletion command to be accepted by Glacier Vault Lock, the following must be met:
        - The retention expiration date must be in the past, as calculated using the longest ArchiveAgeInDays retention period associated with the Vault and the upload date of the Archive record.
        - A "hold" tag must not be associated with the Vault.
- Any attempt by a Root Administrator or other administrators or by an API call to delete a Vault or an Archive (prior to the expiration of the retention period) will be denied once the Vault is successfully locked.
- To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock. The system clock should regularly and frequently (about every one to five minutes) check the time of the external source and resynchronize. This prevents, or immediately corrects, any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of Archive records.

2.1.4 Considerations

The following considerations are provided to establish certain usage and configuration requirements for the broker-dealer and for the Glacier archival storage system to ensure that the conditions of this requirement of the Rule is met.

- To assure that the retention management requirements are met for a Vault with a Vault Lock policy, it is recommended that the broker-dealer:
    - Create a separate Vault for each set of Archive records that have a common time-based retention period. (Each Vault can only have one Vault Lock policy with one

    ArchiveAgeInDays retention period; this policy cannot be shortened or extended; and, therefore, must be carefully assigned to the Vault.)

  - Make the Vault Lock policy immutable (locked), using the CompleteVaultLock API call with the appropriate Lock ID for the Vault.
  - Store the Archive records in a Vault configured with the appropriate retention period.

- Preferably, the Vault Lock policy is applied only to a new (empty) Vault so that any Archive records stored in the Vault are protected for the full retention period.
  - The retention expiration date of each Archive record is calculated using the Archive record upload timestamp and the ArchiveAgeInDays retention period. Therefore, any Archive records that are stored in the Vault prior to applying a Vault Lock policy will be retained only for the remainder of the retention period. For example, Archive records already stored in a Vault 60 days prior to a Vault Lock policy being applied with an ArchiveAgeInDays retention period of 90 days will be protected for only 30 days.
- The clock controlling a Glacier archival storage system must be configured with, or synchronized to, an external time source, such as a Network Time Protocol (NTP) source, to prevent tampering that could result in the premature deletion of an Archive.
- Glacier currently supports only Archive records with time-based retention periods, Archive records requiring conditional (or event-based) retention periods, such as "Life of Client Relationship +6 Years," should not be stored in Glacier.

2.2 Accurate Recording Process

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

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

The intent of this requirement is to ensure both the accuracy and quality of the recording process; making certain that the records read from the storage media are precisely the same as those that were recorded. This requirement includes both a quality verification of the recording process and post-recording verification processes.

2.2.2 Compliance Assessment

It is Cohasset's opinion that the Glacier capabilities, related to the data recording process and the post-recording verification, meet the requirements of the Rule.

2.2.3 Capabilities of Amazon Glacier with Vault Lock

The capabilities described below address the capabilities of Glacier at the time of initial recording and during the post-recording life of the stored Archive records.

2.2.3.1 Recording Process

- A combination of checks and balances in advanced storage recording technology utilized by Glacier (such as advanced magnetic storage technology which utilizes multiple inter-component and inter-step, cyclic redundancy checks (CRCs), as well as write-error detection and correction) are relied upon to ensure that the Archives are written in a high-quality and accurate manner.
- Glacier synchronously stores the Archive record data across multiple facilities (Availability Zones) and multiple storage devices before returning a "stored successfully" response to the uploading application.
- The client application is required to upload a checksum of the Archive record, computed based on the Archive content. Glacier recalculates a checksum from the content of the received Archive record and compares it to the uploaded checksum. If the checksums do not match, Glacier rejects the upload and notifies the client application.
- Additionally, Glacier calculates and stores a checksum in the metadata of each Archive record for use during future retrieval and integrity verification checks.

2.2.3.2 Post-Recording Verification

- As an integral step of the retrieval process, Glacier recalculates the checksum and compares it to the stored checksum to verify the integrity of the Archive record.
- Additionally, Glacier periodically and systematically performs fixity (integrity) checks on each Archive record, by comparing a recalculated checksum to the stored checksum.
- In the event that the checksum comparison identifies an error – during retrieval or the periodic fixity (integrity) checks – Glacier utilizes automatic, self-healing error correction to restore the Archive record to its original state, utilizing the Archive record data stored across multiple Availability Zones (see below).

2.2.4 Considerations

There are no considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

2.3.1 Compliance Requirement SEC 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 SEC's 2001 Interpretive 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 by capturing index data or metadata associated with each electronic record that: (a) *uniquely* identifies the record, and (b) associates the *date and time of recording* with each record.

2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Glacier meet the requirements of the Rule for serializing the original and duplicates of the Archive records.

2.3.3 Capabilities of Amazon Glacier with Vault Lock

- Glacier assigns a unique Archive ID for every Archive record received. Therefore, uploading two Archive records with the same file name will result in two separately stored Archive records with two unique Archive IDs. Specifically, the second Archive record will not overwrite the first one or any previously received Archive records.
- The upload date and time is stored as system metadata for each Archive record. This date is used to calculate the retention expiration date.
- The combination of the unique Archive ID and date/time of recording provide a serialization of each Archive record in both space and time.

2.3.4 Considerations

There are no considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

> *SEC 17a-4(f)(2)(ii)(D): Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.*

This requirement for downloading records and indexes to an acceptable medium is designed to enable the SEC to request a broker-dealer to download the records and associated indexes from the primary storage medium, to a medium acceptable under the Rule, e.g., micrographics or electronic storage media. This allows the SEC or self-regulatory organizations to take possession of the downloaded records and indexes.

2.4.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Glacier meet this requirement of the Rule by providing the capabilities for an administrator or client application to select and download all or some Archive records and associated metadata. Using local capabilities, the downloaded Archive records can be transferred to a medium acceptable under the Rule.

2.4.3 Capabilities of Amazon Glacier with Vault Lock

The Glacier capabilities that support the capacity to download Archives and metadata include:

- Using the unique Archive ID assigned by Glacier when the Archive is stored, the client application can request one or more Archive records to be downloaded from Glacier. Once downloaded, local capabilities may be used to view, reproduce or transfer the records to a medium acceptable under the Rule.
- Additionally, an authorized administrator can request Glacier to download the Vault inventory, which lists the metadata of all Archive records stored in that Vault. Once received, the administrator can select one or more Archive records to be downloaded from Glacier. Once downloaded, the Archive records can be printed or transferred to any medium acceptable under the Rule, using appropriate local application software.

2.4.4 Considerations

The broker-dealer is responsible for authorizing administrative users, which includes privileges to submit Vault inventory retrieval requests.

The broker-dealer is also responsible for submitting the downloaded Archive records and index metadata to the SEC or designated SRO/DEA, as requested.

2.5 Duplicate Copy of the Records Stored Separately

2.5.1 Compliance Requirement SEC 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 records, should the primary source be compromised, i.e., lost or damaged.

Note: A “duplicate copy” is different from a “backup copy.” A duplicate copy is the recording of each record to a second compliant storage system or media, which is then retained for the same period of time as the originally stored record. A "backup copy," in contrast, is typically overwritten as it is “rotated” on a periodic basis, which usually results in a much shorter retention period than the length of time that the original record must be retained.

2.5.2 Compliance Assessment

It is Cohasset’s opinion that the capabilities of Glacier, while not meeting the explicit details of this requirement for storing a complete duplicate copy, meet the intent behind this requirement of the Rule, since Glacier can both (a) access an Archive record when a single storage site fails, and (b) restore an Archive record, when an error is identified.

2.5.3 Capabilities of Amazon Glacier with Vault Lock

- Amazon Glacier synchronously stores Archive record data redundantly in three separate facilities (Availability Zones) and on multiple devices within each facility before returning a “successfully stored” response to the client application.

- Glacier automatically restores Archive records when (a) the recalculated checksum indicates an error with an Archive record, (b) errors on one or more storage devices are detected, or (c) an entire Availability Zone is lost due to a technical or natural disaster.

2.5.4 Considerations

There are no considerations related to this requirement.

3. Conclusions

Cohasset assessed the functionality of Glacier with Vault Lock in comparison to the recording, storage and retention requirements and conditions of SEC Rule 17a-4(f) and the two associated SEC Interpretive Releases, as well as the relevant storage requirements of the CFTC Rule 1.31(b)-(c).

Cohasset determined that Glacier with Vault Lock has the following capabilities, which supports its ability to meet the recording, storage and retention requirements:

- Maintains Archive records in a non-erasable and non-rewriteable format for the *time-based*[4] retention period, assigned by the ArchiveAgeInDays attribute for a locked Vault.
- Preserves Archive records pursuant to a subpoena or legal hold by assigning a legal hold tag to the entire Vault.
- Prohibits deletion of an Archive record until both (a) the ArchiveAgeInDays retention expiration date has passed and (b) the legal hold tag is set to "false".
- Automatically verifies the accuracy and quality of the recording process utilizing (a) advanced storage recording technology (such as magnetic storage); (b) a checksum that is uploaded by the client application with each Archive which is verified by Glacier upon receipt; and (c) a checksum that is generated by Glacier during the recording process which is stored as Archive metadata and utilized for post-recording verification during retrieval and periodic integrity checking.
- Uniquely identifies and chronologically serializes each stored Archive record.
- Synchronously stores Archive record data redundantly in three separate facilities (Availability Zones) and on multiple devices within each facility before returning a "successfully stored" response to the client application; and automatically restores an Archive record when (a) the recalculated checksum indicates an error, (b) errors on one or more storage devices are detected, or (c) an entire Availability Zone is lost due to a technical or natural disaster.

Accordingly, Cohasset concludes that the Amazon Glacier archival storage system, in conjunction with Vault Lock, released in July 2015, when properly configured, meets the five SEC 17a-4(f) and CFTC 1.31(b)-(c) requirements that relate directly to the recording, storage and retention of records required for regulatory compliance.

[4] Time-based retention periods use the creation or storage date to calculate the retention expiration date. As noted in Section 2.1.4, conditional or event-based retention periods, which use a triggering date, are not supported by Glacier.

4. Overview of Relevant SEC and CFTC Requirements

This section establishes the context for the regulatory requirements that are the subject of this assessment by providing an overview of the SEC and CFTC regulatory foundation for allowing electronic records to be retained on a variety of compliant electronic storage media.

4.1 Overview of SEC Rule 17a-4(f) Electronic Storage Requirements

Recordkeeping requirements for the securities broker-dealer industry are stipulated by the United States Securities and Exchange Commission ("SEC") Regulations, including 17 CFR §§ 240.17a-3 and 240.17a-4. Specifically, SEC Rule 17a-4(f), when adopted on February 12, 1997, expressly allowed records to be retained on electronic storage media, subject to meeting certain conditions. Additionally, the Financial Industry Regulatory Authority (FINRA) Rule 4511(c) stipulates:

> *(c) All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA Rule 17a-4.*

Three separate foundational documents collectively define and interpret the specific regulatory requirements that must be met for an electronic storage system to be compliant with SEC Rule 17a-4(f). These are:

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- 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 SEC Rule 17a-4, dated May 1, 2001 (the "2001 Interpretive Release").
- SEC Interpretive Release No. 34-47806, Electronic Storage of Broker-Dealer Records, dated May 7, 2003 (the "2003 Interpretive Release").

In the Rule and in the two subsequent interpretative releases, the SEC authorizes the use of electronic storage media and devices to satisfy the recordkeeping requirements of SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, Rule 17a-4(f)(1)(ii) states:

> *(f) 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.*
> *(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, that meets the applicable conditions set forth in this paragraph (f).*

The 2003 Interpretive Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, meets the requirements of a non-erasable and non-rewriteable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive 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), which are integral to the hardware and software of the recording process, to protect against overwriting or erasure of any records.

Examples of integrated control codes relevant to a non-rewriteable and non-erasable recording process are:

- A retention period during which the record object cannot be erased, overwritten or otherwise modified;
- A unique record identifier that differentiates each record from all other records; and
- The date and time of recording, which in combination with the unique identifier "serializes" the record.

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

Further, the 2003 Interpretive Release requires the storage system to be capable of retaining records beyond the SEC-established retention period, when required by a subpoena, legal hold or other similar circumstances. In *Section IV. Discussion*, the 2003 Interpretive Release states:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules. [emphasis added]*

An important associated requirement of SEC Rule 17a-4(f)(2)(i) is that a member, broker or dealer electing to electronically store its records required by SEC Rules 17a-3 or 17a-4, must notify its designated examining authority at least ninety (90) days prior to employing any technology other than write-once read-many ("WORM") optical media. Examining authorities are self-regulatory organizations (SROs) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

4.2 Overview of CFTC Rule 1.31(b)-(c) Electronic Storage Requirements

Recordkeeping requirements promulgated by Commodity Futures Trading Commission (CFTC) include 17 CFR § 1.31 (CFTC Rule 1.31). When effective on June 28, 1999, CFTC Rule 1.31 authorized entities under the regulatory jurisdiction of the CFTC to retain records on an electronic storage media or system, subject to the requirements and conditions of the Rule. The Commission has modified CFTC Rule 1.31 over time; however, these modifications have not substantively affected the explicit requirements for electronic storage media, which are the basis of this assessment.

However, recent changes to CFTC Rule 1.31(a)-(b), amended in response to The Dodd-Frank Wall Street Reform and Consumer Protection Act and effective January 2, 2013, significantly expanded the requirement for a regulated entity to retain its existing electronic records, which must be kept in *native file format*. CFTC Rule 1.31(b) states:

> *(b) Except as provided in paragraph (d) of this section, books and records required to be kept by the Act or by these regulations may be stored on either "micrographic media" (as defined in paragraph (b)(1)(i) of this section) or "electronic storage media" (as defined in paragraph (b)(1)(ii) of this section) for the required time period under the conditions set forth in this paragraph (b); Provided, however, For electronic records, such storage media must preserve the native file format of the electronic records as required by paragraph (a)(1) of this section. ***** [emphasis added]*

The CFTC Rule 1.31(a)(1) defines *native file format* as:

> ******[N]ative file format means an electronic file that exists in the format in which it was originally created.*

The issue of technology obsolescence and the need to migrate data from its current *native file format* is discussed in the November 2, 2012, Federal Register, which published the amended final rules. Specifically, *II. Comments Received and Amended Regulations*, includes the following excerpts:

> *[T]he Commission is now making clear that paper records are not usable by the Commission as a substitute for the underlying financial data used to create that paper.*
> *Therefore, it is necessary that electronic records be maintained in their native file format and not reduced to paper.*
> *Accordingly, for records that include data stored in a database, the ''native file format'' is the format in which the data is maintained in that database, not a format reduced to paper or imaged format, which is essentially the equivalent of paper.*
> *[T]he Commission confirms that maintaining data in native file format (i.e., the format in which it was originally created or maintained) does not prohibit a recordkeeper from migrating that data from an*

> *obsolete or legacy system or database to a new system or database, where it will then be maintained in the native file format of the new system or database. [emphasis added]*

Accordingly, the CFTC recognizes that the *native file format* may change over time, due to data migrations, for example.

It is important to emphasize that this requirement to retain electronic records in *native file format* does **not** change the requirements of CFTC Rule 1.31(b)-(c) for electronic storage media of the electronic records.

The electronic storage media requirements of CFTC Rule 1.31(b)-(c) are substantively the same as promulgated in the Federal Register on May 27, 1999. Further, these individual requirements are very similar to, and in some cases essentially identical to, the equivalent electronic storage system requirements that are defined in SEC Rule 17a-4(f), including the requirement to "*Preserve the records exclusively in a non-rewriteable, non-erasable format.*" When issuing the final Rule the Commission stated:

> *In view of the significant number of firms subject to regulation under both the federal commodity and securities laws, the final regulations recognize the value of maintaining consistency, where possible, between the Commission's approach to recordkeeping and that of the SEC. The regulations do not reflect strict conformity with the regulations the SEC adopted in 1997, however, because the Commission concluded that there were significant differences between the commodities and securities industry that justified retaining certain of its current rules.*

To evaluate the applicability of the SEC's Interpretive Releases, including authorized use of erasable and rewritable media, to the recordkeeping requirements of the CFTC, Cohasset reviewed the information published in the May 27, 1999, Federal Register. This Federal Register published the CFTC's adoption of the amendments to CFTC Rule 1.31 and contained the following excerpt in the *Supplementary Information*:

> *On several occasions during the past two years, the Commission has provided interim relief from the current requirements of Rule 1.31 to Commission registrants using advanced technology(44).*

In footnote (44), the Commission states:

> *The Commission has permitted these registrants to substitute compliance with the SEC's recordkeeping requirements for compliance with current requirements of Rule 1.31 ******

This footnote describes the CFTC's willingness to rely, where appropriate, on the SEC's rules and its history of granting permission to alternatively substitute compliance with the SEC's recordkeeping requirements, for compliance with the requirements of CFTC Rule 1.31. This suggests that it is reasonable to conclude that the CFTC would accept compliance with the SEC 2003 Interpretive Release as a substitute for, or a complement to, the Commission's rulemaking related to CFTC Rule 1.31(b)-(c).

In the *Supplementary Information* provided with CFTC Rule 1.31, the CFTC also acknowledges that registrants would benefit from the use of evolving storage media and technology, by stating:

> *The Commission recognizes the important role improved technology can play in the continued development of the futures industry. Minimizing unnecessary regulatory obstacles to the [adoption] of improved technology is a goal of industry members, customers, and the Commission.*

One basic difference between the CFTC Rule and the SEC Rule, is that the CFTC Rule only requires notification to the Commission prior to placing a compliant system into production. The SEC Rule, however, requires the regulated entity to send a notification letter to the appropriate Designated Examining Authority (DEA) ninety (90) days prior to deploying a compliant non-WORM system.

Even though the CFTC has not issued any formal interpretive releases or statements subsequent to the effective date of CFTC Rule 1.31, nor have they indicated direct support of the SEC's 2003 Interpretive Release, it is Cohasset's opinion that the CFTC would interpret the use of advances in digital storage media and systems technology (such as erasable magnetic storage using the integrated control codes stipulated in the 2003 SEC Interpretive Release) as compatible with the vision and intentions of the CFTC for CFTC Rule 1.31(b)-(c).

Also see the following section for a comparison of the storage requirements of the SEC and CFTC Rules.

4.3 Comparison of Relevant Requirements of SEC and CFTC Rules

The individual relevant requirements cited in the body of this report are based on the wording in SEC Rule 17a-4(f). The SEC requirements that are cited in this report are very similar in number, principal and context, if not always in their wording, to requirements stated in CFTC Rule 1.31(b)-(c).

For cross reference, the table below provides a one-for-one comparison of the relevant recording, storage and retention requirements of SEC Rule 17a-4(f) with the similar requirements of CFTC Rule 1.31(b)-(c).

The following requirements reflect the most recent updates to SEC 17a-4(f)(2)(ii)(A)-(C) and CFTC 1.31(b)(1)(ii)(A)-(C).

SEC 17a-4 Requirement		CFTC 1.31 Requirement	
(f)(2)	If electronic storage media is used by a member, broker, or dealer, it shall comply with the following requirements:	(b)	Except as provided in paragraph (d) of this section, books and records required to be kept by the Act or by these regulations may be stored on either "micrographic media" (as defined in paragraph (b)(1)(i) of this section) or "electronic storage media" (as defined in paragraph (b)(1)(ii) of this section) for the required time period under the conditions set forth in this paragraph (b); Provided, however, For electronic records, such storage media must preserve the native file format of the electronic records as required by paragraph (a)(1) of this section.
(f)(2)(ii)	The electronic storage media must:	(b)(1)(ii)	The term "electronic storage media" means any digital storage medium or system that:
(f)(2)(ii)(A)	Preserve the records exclusively in a non-rewriteable, non-erasable format;	(b)(1)(ii)(A)	Preserves the records exclusively in a non-rewritable, non-erasable format;
(f)(2)(ii)(B)	Verify automatically the quality and accuracy of the storage media recording process;	(b)(1)(ii)(B)	Verifies automatically the quality and accuracy of the storage media recording process;

SEC 17a-4 Requirement		CFTC 1.31 Requirement	
(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; and	(b)(1)(ii)(C)	Serializes the original and, if applicable, duplicate units of storage media and creates a time-date record for the required period of retention for the information placed on such electronic storage media; and
(f)(2)(ii)(D)	Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.	(b)(1)(ii)(D)	Permits the immediate downloading of indexes and records preserved on the electronic storage media onto paper, microfilm, microfiche or other medium acceptable under this paragraph upon the request of representatives of the Commission or the Department of Justice.

The following requirements reflect the most recent updates to SEC 17a-4(f)(3)(iii) and CFTC 1.31(b)(2)(iv).

SEC 17a-4 Requirement		CFTC 1.31 Requirement	
(f)(3)	If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:	(b)(2)	Persons who use either micrographic media or electronic storage media to maintain records in accordance with this section must:
(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.	(b)(2)(iv)	Store a duplicate of the record, in any medium acceptable under this regulation, at a location separate from the original for the period of time required for maintenance of the original; and

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is one of the nation's foremost management consulting firms specializing in records management and information governance. Spanning 40 years and serving both domestic and international clients, Cohasset provides award-winning professional services in four areas: management consulting, education, thought-leadership and legal research.

Management Consulting: Working with multi-national clients, Cohasset develops effective records and information management programs that promote interdisciplinary governance. Cohasset also engages in implementation activities to achieve business goals, improve compliance and mitigate risk. Distinguished as a leader of the transition from records management to information governance, Cohasset held its first Managing Electronic Records (MER) Conference in 1993. Cohasset's current and former clients include several winners of ARMA's prized Cobalt Award. Cohasset is proud of its reputation for attaining exceptional results.

Education: Cohasset is renowned for its longstanding commitment to education on information governance and records and information lifecycle management.

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete unneeded information*
- *Designs and assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

Thought-Leadership: Cohasset regularly publishes thought-leadership white papers and surveys to promote continuous improvement in the lifecycle management of information.

Legal Research: Cohasset is nationally respected for its direction on records and information management legal issues – from retention schedules to compliance with regulatory requirements associated with the use of electronic or digital storage media.

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, which, combined with its commitment to excellence, has resulted in Cohasset's extraordinary record of accomplishments and innovation.