Immutable Data Lock Backup For FINRA-SEC Compliance

The financial services sector has to comply with a whole different level of regulations. Prominent amongst them is the *Financial Industry Regulatory Authority* (FINRA) compliance. Compliance with regulations has to also extend to third-party software and applications that the financial organization employs. In this blog, we discuss the compliance requirements for backup solutions, particularly FINRA SEC 17a-4.

The FINRA-SEC Regulations Discussed

Here are the three key rules of the FINRA-SEC Regulations that we will touch upon:

- **Securities and Exchange Commission (SEC) Rule 17 CFR 240.17a4(f)** regulates exchange members, brokers, or dealers. They stipulate recordkeeping requirements, including retention periods and type of storage technology.
- **Financial Industry Regulatory Authority (FINRA) Rule 4511(c)** requires that all records comply with the format and media requirements of SEC Rule 17a-4(f).
- **Commodity Futures Trading Commission (CFTC) Rule 17 CFR 1.31(c)-(d)** refers to the form and manner in which regulatory records must be retained.

Immutable Data Backup For FINRA-SEC 17a-4 Compliance

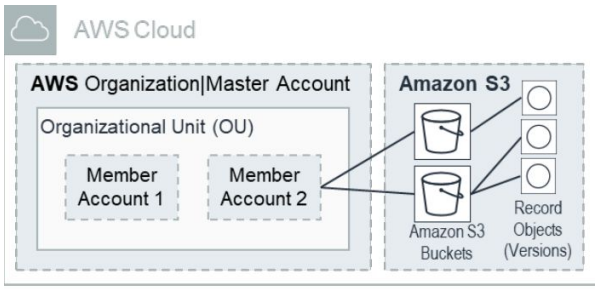
Immutable backups have data stored using a *write-once-read-many* (WORM) model. This "locks" the backed up data and prevents it from being modified, corrupted, or deleted.

Backups with immutable data locks help you meet regulatory requirements that require WORM storage, and add another layer of protection against object modifications and deletion. They further your organization's compliance with FINRA SEC 17a-4 regulations.

CloudAlly's Immutable Data Backup With S3 Object Lock (BYOS Only)

CloudAlly has provided secure (and unlimited) Amazon S3 storage for daily backups since it pioneered SaaS backup almost a decade ago. Our backups have always been immutable and cannot be modified or changed by users. Immutable backups are your company's best defense against a ransomware attack, as they guarantee easy and accurate data recovery.

However, as the customer has full control of the data, the account administrator ultimately can delete backup tasks as required, in the capacity of their account management role. Our latest product release adds an extra layer of security with Object Lock, an explicit data backup lock. **Note: Object Lock can be applied *only* when the backups are on the client's own storage (BYOS: Bring Your Own Storage)**. S3 Object Lock is an Amazon S3 feature that ensures that backups cannot be changed or deleted until a customer-defined retention period has elapsed. It retains records in a non-rewritable and non-erasable format and meets the relevant storage requirements set forth in the data regulations listed above. The S3 Object Lock feature has been independently assessed for use by financial companies that are subject to FINRA, SEC 17a-4, and CTCC regulations.



Hierarchy of AWS services (source: Amazon)

Note, that once Object Lock is turned on, it cannot be turned off and backups cannot be removed for any reason until the retention period expires. Contact support for further information on how to activate this feature.

Secure and Compliant Backups with CloudAlly

Apart from the Immutable Storage or Object-Lock capability, our secure credentials are impeccable.

- We're ISO 27001 certified, HIPAA and GDPR compliant
- We support MFA/2FA authentication and OAuth permissions
- Our backups are on stringently secure Amazon S3 (unlimited storage is included)
- Backup data is encrypted at-rest and in-transit with advanced AES-256 bit encryption.

Protect your business-critical data with secure, compliant, and immutable data backups with CloudAlly