



Piler Enterprise for Financial Services

Email Archiving for SEC/FINRA Compliance

The Challenge

Financial services firms face stringent email retention requirements:

- **SEC Rule 17a-4:** 6-year retention, 2 years immediately accessible
- **FINRA Rules 3110/4511:** Supervision and retention requirements
- **SOX Section 802:** 7-year retention for audit-related communications
- **Immutability:** Records must be non-rewriteable, non-erasable (WORM)
- **Rapid Production:** Regulators expect quick responses to requests

Non-compliance penalties can reach millions of dollars plus reputational damage.

How Piler Helps

Requirement	Piler Capability
6-7 Year Retention	Configurable retention policies with legal hold
Immutable Storage	Write-once archive, cryptographic integrity
Rapid Search	Sub-200ms search (typical), instant regulatory response
Audit Trails	Complete logging of all access and exports
Supervision	Search and review capabilities for compliance
Data Sovereignty	Self-hosted - no third-party cloud exposure

Regulatory Compliance Features

SEC Rule 17a-4 Requirements

Requirement	Piler Implementation
Preserve records for 6 years	Configurable retention policies
First 2 years immediately accessible	All records searchable in < 200ms (typical)
Non-rewriteable, non-erasable	Immutable storage, integrity verification
Separate copies	Built-in backup/replication support
Index and retrieve by date	Full date-range search capabilities

FINRA Supervision

- Search employee communications by keyword, date, sender
- Export for review and documentation
- Audit trail for supervision activities

Smart Insights: Automated Risk Detection

Piler's scanner automatically flags emails containing:

- **Credit card numbers** - PCI-DSS relevant
- **Social Security Numbers** - Identity theft risk
- **IBAN/Account numbers** - Financial data exposure
- **Custom patterns** - Configure for your risk indicators

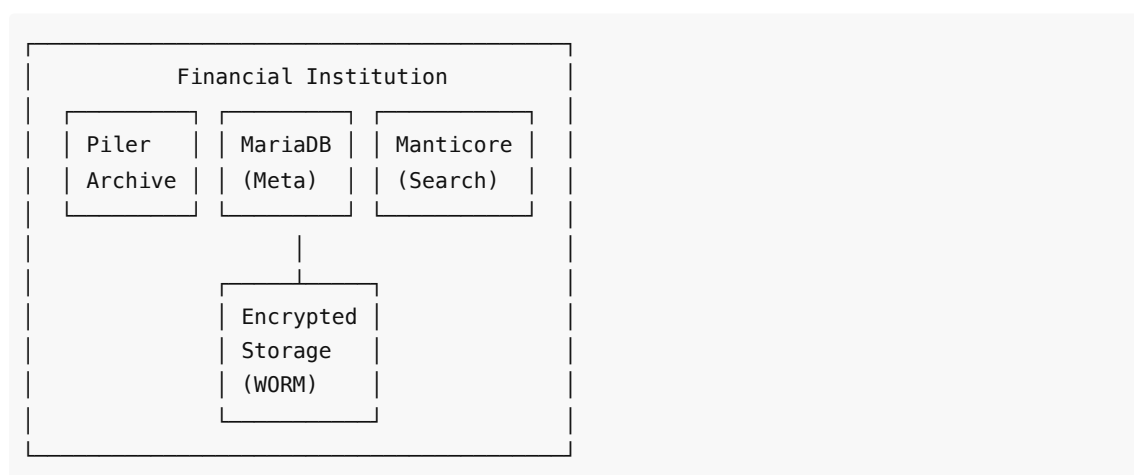
Compliance teams receive prioritized alerts for review.

Why Self-Hosted for Financial Services?

Concern	Cloud Archiving	Piler Enterprise
Regulatory Control	Vendor dependency	Direct control
Exam Readiness	Request from vendor	Instant access
Data Location	Vendor's infrastructure	Your data center
Vendor Risk	Third-party exposure	Eliminated
Exit Strategy	Vendor lock-in	Full data ownership

Examiners prefer organizations that control their own compliance data.

Deployment Architecture



All components on your infrastructure - no external dependencies.

Compliance Reporting

Built-in dashboards for:

- Archive health and completeness
- Storage utilization and growth
- User access patterns
- Search and export activity

Export capabilities for:

- Regulatory exam documentation
 - Internal audit reports
 - Supervision records
-

Client Talking Points

"SEC Rule 17a-4 requires immutable email retention. Basic backup isn't compliant."

"FINRA audits? One-click compliance reports and instant search."

"7-year retention with guaranteed integrity - no third-party risk."

"When examiners arrive, you have immediate access. No vendor delays."

Exam Readiness Checklist

- ☐ All email automatically archived (journal/BCC)
- ☐ Retention policies configured per regulation
- ☐ Legal holds available for investigations
- ☐ Search < 2 minutes for any date range
- ☐ Export capability for production
- ☐ Audit logs for access documentation
- ☐ Backup/DR plan documented

Piler addresses all checklist items.

Next Steps

1. **30-Day Free Trial** - Test regulatory search scenarios
2. **Compliance Demo** - Walk through exam-readiness features
3. **Architecture Review** - Design compliant deployment

Contact: partners@mailpiler.com | <https://mailpiler.com/partners>

Piler Enterprise is designed to help financial services firms meet email retention requirements. Consult your compliance officer and legal counsel for firm-specific regulatory guidance.