

# PROOFPOINT ENTERPRISE ARCHIVE FOR SEC AND FINRA COMPLIANCE

## PROOFPOINT PROVIDES FINRA AND SEC REGULATED FIRMS WITH:

- **Simplified regulatory compliance.** Helps firms to meet regulatory requirements by archiving all messages and content according to compliance retention policies. Enables staff to systematically review messages for compliance supervision.
- **Enhanced compliance team efficiency.** Provides a single, unified interface to for electronic communications including email, IM, Bloomberg, voice, SMS, enterprise collaboration and social content. Search performance improves productivity and provides quick responses to regulatory inquiries.
- **Uncompromised data protection.** Robust information control and unsurpassed cloud data privacy protection.

## THE LEADING CLOUD SOLUTION DESIGNED FOR BROKER-DEALERS AND INVESTMENT ADVISORS

With Proofpoint Enterprise Archive, you get the most secure, powerful and cost-effective solution available for compliance, supervision and legal discovery. It allows financial organizations to govern and discover a wide range of data. This includes email, instant message conversations, enterprise collaboration content, social media, text, voice and more. And with all data managed to address all requirements outlined by SEA 17a3-4. We also provide a proven Supervisory Review module to manage the selection and review of communications in accordance with Financial Services mandates established by Financial Industry Regulatory Authority (FINRA), Securities and Exchange Commission (SEC), and Investment Industry Regulatory Organization in Canada (IIROC).

### Why Proofpoint?

Today, financial services firms are constantly challenged by the demands of the business to enable the use of exploding numbers of communications channels, increasingly rigorous regulatory requirements, and complex and disruptive e-discovery demands. This is in addition to the on-going task of managing ever-expanding data volumes and locations. Proofpoint was founded with a singular focus of helping organizations protect critical information, and has established itself as the leading cloud provider that enables organizations to defend, protect, archive and govern their most sensitive data. This is demonstrated by our financial services customers, many of whom are archiving more than 1 billion items and successfully meeting regulatory and legal obligations around the world. Excellent customer service ratings and 90+% customer retention rates clearly demonstrate that Proofpoint—unlike many other cloud providers—was designed for those with complex regulatory and e-discovery demands.

### Single Pane of Glass

Proofpoint Enterprise Archive provides a single, unified interface. It allows you to retain, preserve, discover and review email, instant message conversations, enterprise collaboration content, social media, text, voice and more quickly and efficiently. Whether you're addressing a FINRA inquiry, preparing for litigation, or simply accessing your own historical content, we deliver information consistently now and over time as information volume continues to grow—which we uniquely back with a search performance service level agreement (SLA).

### Compliance. Simplified.

Proofpoint provides a fully-managed service that ensures that information is always accessible for quick and easy search and retrieval, which enables efficient regulatory response. Data integrity is assured, beginning with Proofpoint's "pull-and-confirm" method of information capture. This guarantees that all items have been successfully archived before removing them from the journaling process. Optionally, Proofpoint Compliance Gateway can also ensure that your content is properly retained. As additional insurance, it has a built-in feedback loop to

confirm that the archive successfully processed each message from your content sources. If not, it will resend the data. Compliance Gateway can also be used to filter and route content to multiple destinations. Ongoing integrity is maintained by a digital fingerprinting process that ensures MD5 values match those stored at the time of archiving. All searches, message views, exports, retrievals and supervisory activities are tracked with complete audit trails and comprehensive reporting. This provides you with complete visibility into compliance tasks, who performed them, and when.

**Innovative, Cloud-Based Service Delivery**

Enterprise Archive is delivered via an innovative, SSAE-16 certified cloud architecture with jurisdictional assurance provided via paired and geographically-distributed data centers located in the United States, Canada, the Netherlands, and Germany. Data is maintained in accordance with all conditions set forth in SEC Rule 17a-4 as further described in the following section.

**Uncompromised Data Security and Privacy**

With patented Proofpoint DoubleBlind™ Key Architecture, all messages, files and other content are encrypted with keys controlled by the customer before data reaches the Proofpoint data centers. This ensures that no one can access a readable form of customer data without authorized access by the customer to the encryption keys stored behind the customer firewall. This also ensures that customer data is always encrypted.

**PROOFPOINT AND SEC 17A-4 REQUIREMENTS**

Beyond the archiving process, we leverage our information security leadership to address all conditions set forth in SEC Rule 17a-4. The table below summarizes how Proofpoint addresses each specific section of SEC 17a-4:

SEC Rule 17a-4 Requirement	How Proofpoint Addresses
17a-4 (a) Every member dealer must preserve business records for at least 6 years. The first 2 years must be easily accessible.	
(f) Retain records for three to six years (depending on the type of record), the first two years in a readily available location.	Enables classification and retention of any/all messages on either a global policy or granular policy basis.
(f)(2)(ii)A Preserve all electronic records in a non-rewritable and non-erasable format.	Stores multiple copies of messages and indexes on SEC 17a-4 compliant storage.
(f)(2)(ii)(B) Automatically verify the quality and accuracy of the storage media recording process.	Checks the digital fingerprint of messages to verify quality and accuracy of the recording process
(f)(2)(ii)(C) Store a duplicate copy of records separately from the original for the specified retention period. 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.	Stores multiple copies of each message on different equipment within the primary data center. An additional copy is stored at a secondary data center. Messages have a unique MD5 hash and can be stamped with an applicable retention period.
(f)(2)(ii)(D) Organize and index all original and duplicate copies of records. Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member	Indexes all information submitted for storage. The index information is replicated to each location where data is stored.
(f)(3)(v) Put in place an audit system providing for accountability regarding inputting of any changes made to every original and duplicate record maintained	Indexes all information submitted for storage. The indexed information is replicated to each location where data is stored. Data can be exported to a variety of formats.

SEC Rule 17a-4 Requirement	How Proofpoint Addresses
(f)(3)(vi) Have ready to produce upon request all information needed to access records and indexes.	Provides access to all information stored. Search performance guaranteed by SLAs.
(f)(3)(vii) Ensure a third-party has access to and the ability to download a firm’s records.	Proofpoint can serve as designated third party should SEC request copies of archived data. Proofpoint presents proof of the SEC request to key escrow service provider. Copies of the encryption keys to are released to Proofpoint. Requested data is then exported to the SEC.

**BROKER DEALER AND INVESTMENT ADVISOR REQUIREMENTS**

In addition to addressing all SEC 17a-4 requirements, Proofpoint enables FINRA regulated broker-dealers and SEC-regulated investment advisors (including hedge funds and private equity funds) to address specific record keeping, supervisory, and audit/reporting requirements as summarized below:

FINRA: Broker-Dealer Requirements	How Proofpoint Addresses
<p><b>Record Keeping: FINRA Rule 4511</b> based on NASD Rule 3110(a) and NYSE Rule 440, firms are obligated to: (1) preserve books and records as required under the rules of FINRA, the Securities Exchange Act (SEA) and applicable SEA rules; and (2) preserve records required under FINRA rules in a format and media that complies with SEA Rule 17a-4. Archive Instant messages pursuant to NASD Notice to Members on Instant Messaging, July 2003.</p>	<p><b>Enterprise Archive</b> allows organizations to preserve email, IM, Bloomberg, voice, SMS, enterprise collaboration and social content, for a period of at least six years per requirements of the FINRA rules in SEA 17a-4.</p>
<p><b>Communications with the Public: FINRA Rule 2210</b> Firms must retain communications and correspondence with the public pursuant to SEA Rule 17a-4 and 17a-(b).</p>	<p><b>Enterprise Archive</b> allows organizations to preserve email, IM, Bloomberg, voice, SMS, enterprise collaboration and social content, pursuant to SEA Rule 17a-4 and 17a-(b).</p>
<p><b>FINRA Regulatory Notice 11-39 (Social Media Websites):</b> obligations to preserve social media depend on whether the content constitutes a business communication. Rule 17a-4(b) requires broker-dealers to preserve records for a period of not less than three years, the first two in an easily accessible place (clarifies FINRA Regulatory Notice 10-06)</p>	<p><b>Enterprise Archive</b> allows organizations to capture social content that constitutes a business communication in order to deliver to an archiving that addresses SEA 17a-4(b) requirements.</p>
<p><b>Supervision: FINRA Rule 3110</b>, effective December 2014 (replacing NASD rule 3010), requires firms to:</p> <ul style="list-style-type: none"> <li>a) Establish and maintain a system to supervise activities of associated persons in accordance with FINRA rules.</li> <li>b) Review and evidence review of correspondence and internal communications.</li> <li>c) Retain internal communication and correspondence for the period of time and accessibility specified in SEA 17a-4(b) (internal communications added by FINRA Rule 2210).</li> <li>d) Supervise instant messages pursuant to NASD Notice to Members on Instant Messaging, July 2003.</li> </ul>	<p><b>Intelligent Supervision</b> allows organizations to implement a supervisory system to identify, review and address incoming and outgoing email, IM, Bloomberg, voice, SMS, enterprise collaboration and social media communications; maintain audit trails and records of supervisory reviews; monitor and evaluate supervisory procedures to ensure compliance, and retain internal communication and correspondence for the 3- and 6-year retention periods outlined by SEA 17a-4(b).</p>

SEC: Investment Advisor Requirement	How Proofpoint Addresses
<p><b>Record Keeping: SEC Rule 204-2</b> Investment Advisors Act Rule 204-2 requires Investment Advisors (including Hedge Funds and Private Equity Firms, per Dodd Frank) to preserve all SEC-mandated records, including all written communications; store records on tamperproof media; retain records in easily accessible place for a 5 year retention, arrange and index record for easy search, retrieval and access; furnish records within 24 hours; provide regulators with a means to access, view, and print records.</p>	<p><b>Enterprise Archive</b> allows organizations to preserve email, IM, Bloomberg, voice, SMS, enterprise collaboration and social content within an immutable, tamperproof repository with the ability to retain information in accordance within the 5-year retention period. Our unique grid-based storage architecture also ensures that information is available for immediate access by compliance team or regulator.</p>
<p><b>Supervision: SEC Rule 206(4)-7</b> (along with SEC Final Rule IA-2204 and Rule 204-2(g)3) requires firms to establish supervisory policies; implement safeguards to protect client record privacy; monitor accuracy of disclosures made to investors, clients and regulators; implement controls for record maintenance that secures them from unauthorized alteration; and implements review system with ability to store review results.</p>	<p><b>Intelligent Supervision</b> allows organizations to implement a supervisory system to identify, review and address incoming and outgoing email, IM, Bloomberg, voice, SMS, enterprise collaboration and social media; maintain audit trails and records of supervisory reviews; monitor and evaluate supervisory procedures to ensure compliance; and retain internal communication and correspondence for the 5 year retention periods outlined by SEC 204-2.</p>

**PROOFPOINT AND IIROC (CANADA)**

IIROC Requirement	How Proofpoint Addresses
<p><b>Record Keeping</b></p>	
<p><b>IIROC Rule 29.7:</b> requires firms to monitor, review and archive (for two to five years) electronic advertisements, sales literature and correspondence. All records must be readily available.</p> <p><b>IIROC Notice 11-0349:</b> firms must retain all advertisements and sales literature for 2 years and correspondence with the public for 5 years.</p>	<p><b>Enterprise Archive</b> allows organizations to preserve email, IM, Bloomberg, voice, SMS, enterprise collaboration and social content within an immutable, tamperproof repository with the ability to retain information in accordance with the mandated retention periods.</p>
<p><b>Supervision</b></p>	
<p>Under <b>IIROC 29.7</b> and <b>IIROC Notice 11-0349</b> firms must establish written supervisory procedures, training and monitoring systems for all electronic communications (including social media). Interactive content (e.g. Tweets) must be supervised, but not necessarily pre-approved.</p>	<p><b>Intelligent Supervision</b> allows organizations to implement a supervisory system to identify, review and address incoming and outgoing communications; maintain audit trails and records of supervisory reviews; monitor and evaluate supervisory procedures to ensure compliance; and retain internal communication and correspondence for the mandated retention periods outlined by IIROC 29.7 and 11-0349.</p>

### Third-party downloader service

Upon request, Proofpoint can serve as the Designated Third-Party downloader. In the event that a customer is unable to comply with SEC requests for archived data, and the SEC requests copies of the archived data from Proofpoint, Proofpoint can present proof of the SEC request to a key escrow service provider who releases copies of the encryption keys to Proofpoint. Requested data is then exported to the SEC. Please note that this service requires that the customer's encryption key be enrolled in an escrow account. The escrow service is free for all Proofpoint archiving customers.

### Flexible, yet powerful policy management to meet record keeping requirements

Proofpoint Enterprise Archive makes it easy for you to meet even the most complex regulatory compliance demands. We enable the creation of granular policies based upon classes of users, categories of content, or unique geographic requirements. You can easily define and automatically enforce the data retention and destruction policies necessary to comply with FINRA, SEC and other global financial service mandates or internal policies. Key Policy Management features provide you with:

- Flexibility to easily adjust policies as regulatory or legal requirements change
- Fully transparent policy history to track and report on every policy change in unalterable form
- Tight integration with Microsoft Active Directory to define policies based upon defined user groups
- InfoTags to mark specific items for specific treatment, such as communication between legal teams marked as Privileged

### Quickly and easily meet FINRA, SEC and IROC supervisory requirements

The Proofpoint Intelligent Supervision module allows you to automate review processes. This improves the productivity of your compliance staff and your effectiveness in identifying and routing potential policy violations that require further review or escalation. And our self-service search and near real-time information retrieval—uniquely backed by a performance guarantee—significantly improve the efficiency of the compliance audit process. Proofpoint Intelligent Supervision allows your organization to:

- Specify enforcement rules for each policy item based on the content of communications and attachments, sender role, department and more
- Capture, index, and archive email, social media, instant messages and chat, SMS, voice, enterprise collaboration and Bloomberg content rules according to defined policies, and ensure that information is fully accessible for search and supervisory review
- Monitor the progress of review using real time dashboards to identify review teams that are falling behind
- Monitor and ensure that all reviewers are completing their assigned review work on time
- Inform reviewers and compliance teams when queues grow beyond set thresholds
- Group and review of related messages in a single step with conversation threading
- Demonstrate the history of rules, supervised employees and reviewers at any point in time using policy tracking
- Prove compliance with your stated policy with Evidence of Supervision reports
- Easily export the full history of review activities and comments to auditors in the industry-standard format
- Pre-approve content that is known to be safe in the Content Library to avoid false positives
- Randomly sample a percentage of each user's mail or messages that match specific criteria, rather than just a percentage sample of the entire company's mail
- Assign flagged messages to be reviewed by individual reviewers or by a central resource
- Improve productivity by setting up review workflow scenarios that direct policy violations to subject matter experts
- Find related features to easily search for similar items
- Review by use of "hot keys" to allow for efficient review queue processing by power users
- Preview summaries of potential issues to optimize message review
- Review queue status in real time and reports that reveal the effectiveness of the supervision process

### Sustainably fast information access backed by SLA

Proofpoint provides a search performance guarantee that searches are returned in 20 seconds or less—regardless of how large the archive grows or how often searches are required. Through a web-based user interface, your compliance staff can easily meet even the most stringent compliance audit requirements. Search features allow you to:

- Conduct full-text searches of email and over 400 types of attachments
- Easily find relevant data with highlighted search words
- Include or exclude specific types of content, such as social media, instant messages, or collaborative from search results
- Save frequently used search criteria
- Export search results as EDRM XML, CSV, Relativity Load File or PST files
- Enable broader regulatory information access as required to address regulatory inquiries

### Extended content control

Proofpoint extends the control of financial compliance processes by providing a reconciliated messaging view comprised of email, social media, IM, voice, SMS and a number of additional communication sources. We capture content from the source, convert it to email form, extract text for full searchability, apply applicable policies, and securely store content within our 17a-4 compliant Enterprise Archive. All content then can be searched, preserved and supervised with performance backed by our Search Performance SLA.

#### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.