gamechanger Game Changing Technology for Financial Services Email

Stay Within the Lines: Enforcing Compliant Electronic Communications in Financial Services

By Brien M. Posey

Legal, Compliance and IT professionals working in Financial Services need to focus on these three key areas.

Regulatory compliance has long been one of the single greatest challenges for companies in the Financial Services industry. This is especially true for those regulations that are related to data archiving and the various aspects of data lifecycle management. Although it is impossible to discuss all applicable regulatory requirements within the confines of a single paper, Legal, Compliance and IT professionals working in the Financial Services industry often find that many of the regulatory requirements tend to focus on three key areas.

RECORDKEEPING

The first area to consider is recordkeeping. The Securities and Exchange Act (SEA) outlines numerous recordkeeping requirements that financial services firms must adhere to. For example, Rule 17a-3 requires broker-dealers to make and retain certain records and Rule 17a-4 specifies the length of time and the manner in which these records and other records must be maintained. Meaning, firms must retain blotters containing all purchases and sales of securities for at least six years. But they must keep copies of confirmations for only three years. For the first two years, these records must be kept in an easily accessible place. If it is a business record, it needs to be preserved, regardless if it is an email, chat or tweet.

Although these recordkeeping requirements seem relatively simple on the surface, compliance tends to be both difficult and costly because businesses use so many different communications mediums. A solution that captures and archives email communications for example, might not necessarily be able to capture other forms of electronic communications such as instant messages, or communications that have occurred through social media channels.

Painterr / Shutterstock.com

eDISCOVERY

A second area of focus is eDiscovery. Simply put, eDiscovery is the ability to query an organization's data in an effort to uncover potential relevant data upon request. eDiscovery is performed in response to investigations (both internal and external), litigation, a subpoena, or an audit.

At least some of the challenges associated with eDiscovery are similar to those of recordkeeping in general. Because eDiscovery requirements usually span multiple data types and communications streams, it can be difficult to achieve comprehensive eDiscovery capabilities through a single tool.

Admittedly, some progress has been made in recent years. Microsoft Office

365 for example, includes an eDiscovery tool that can perform eDiscovery across multiple data sources such as Exchange Online and SharePoint Online. Even within Office 365 however, there can be significant amounts of data that fall outside of the scope of the built-in eDiscovery tool. Furthermore, the Office 365 eDiscovery engine is incapable of performing eDiscovery of data residing on non-Microsoft platforms.

The other big problem associated with eDiscovery is that it is most commonly performed in response to litigation. Companies must be able to ensure not only that their eDiscovery efforts are thorough, but also that any data meeting the eDiscovery criteria is placed into a legal hold. Legal hold happens when litigation is reasonably anticipated. This means that if you expect a lawsuit but nothing has been filed yet, you have the legal obligation to actually put all potential relevant data on hold until the matter is resolved. If you wait until the litigation happens and you knew, you are potentially liable. The completeness of the index is also extremely important. Limited filetype support is extremely risky with eDiscovery.

A legal hold excludes designated data from the normal data lifecycle management process. Imagine for example, that an organization uses an automated policy engine to automatically delete old email messages after seven years. If a particular aging email message was the subject of an ongoing legal proceeding, then deleting that message could constitute a crime. As such, a legal hold could be used to prevent the message from being automatically deleted. Legal hold is used to prevent the destruction of potential evidence.

Although the previous example focused on message deletion by an automated policy, that is only one of the ways in which legal holds protect data. A legal hold will commonly also prevent a user from deleting or modifying data that has been placed on hold.

Needless to say, eDiscovery and subsequent legal holds can be expensive. The first pass on content on eDiscovery is ECA (Early Case Assessment) which is used to cull down the data before it goes through a review platform. The handoff of the data through the different stages is also important as it requires chain of custody and full audit reports available (something that Office 365 doesn't offer beyond 90 days).

SUPERVISION

A third challenge that is faced by those working in the financial services industry is that of supervision. The Financial Industry Regulatory Authority (FINRA) defines a number of different rules pertaining to supervisory responsibilities. In short, broker dealers may employ risk based principles to review incoming, outgoing and internal electronic communications to ensure that their associated persons are complying with FINRA rules and federal securities laws.The actual requirements are outlined in sections 3110, 3120, 3130, 3150, 3160, and 3170 of the FINRA rules.

Being that these rules are primarily related to supervisory responsibilities, they would at first seem to be beyond the scope of anything that might be applicable to the IT department. Even so, the IT department's job is to use technology to solve business problems. Some of the supervisory responsibilities could potentially be made easier through the use of IT solutions.

A classic example of how technology can help in this area has to do with the review process that is required for certain types of communications. Any time that a piece of digital content needs to be sent to a client, social media account, public relations firm, etc., that content must undergo a compliance review. Because the compliance requirements may be strict, the compliance team likely finds itself bombarded by content review requests, and can easily begin to accumulate a backlog.

Because the compliance requirements may be strict, the compliance team likely finds itself bombarded by content review requests.

The problem with manually reviewing digital content is that it is a labor intensive process that simply does not scale. As the volume of content that needs to be reviewed increases, so does the workload of the reviewers.

While there will probably always be a need for human reviewers, software can conceivably help with the review process. For example, an automated solution might keep track of the content review queues, so as to help financial services organizations to spot inefficiencies in the review process. By digitally tracking and logging the review process, it may also be easier to prove to regulators that content has been reviewed prior to distribution.

Another problem with manually reviewing content is that in some cases, time may be wasted due to duplicate efforts. If an organization has pre-approved content for distribution, then there is no reason why that content has to be reviewed again. An automated solution could save time by skipping over content that has already received the necessary approval.

Proofpoint's Game Changing Solutions

Helping financial services firms adhere to regulatory requirements

Organizations working within the financial services industry face complex, and rapidly changing government regulations. Among the most stringent of these regulations are those requiring financial services firms to archive and retain electronic communications, and to make those archived conversations available to regulators and auditors upon requests. The difficulty of complying with these requests is compounded because financial services firms routinely use multiple forms of communications both internally, and to engage with investors.

Proofpoint offers solutions to help financial services firms adhere to regulatory requirements, while also making it easier for those firms to grow their business. The three pillars of Proofpoint's approach include recordkeeping, eDiscovery, and Supervision

Of these three pillars, recordkeeping is arguably the most complex because archiving requirements span multiple, disparate systems. Proofpoint's approach to recordkeeping is to implement automated, policy driven content retention that spans all content areas, including social media. Proofpoint can help organizations to archive and classify social media content for use in future compliance and eDiscovery efforts.

PROOFPOINT eDISCOVERY

The second pillar of Proofpoint's approach is eDiscovery. The Proofpoint e-Discovery and Analytics solution is designed to streamline the review process, while also reducing costs. Because Proofpoint archives data to a centralized location, its eDiscovery engine is able to search the full contents of the archives in a single operation, as opposed to requiring reviewers to perform parallel searches of disjointed systems. The system is so efficient that the Proofpoint eDiscovery engine is able to search through hundreds of millions of records in mere seconds.

Just as important, Proofpoint takes steps to minimize the effort required to review the results of an eDiscovery operation.

PROOFPOINT INTELLIGENT SUPERVISION

The third pillar to Proofpoint's approach to helping financial services firms is supervision. Proofpoint's Intelligent Supervision is designed to reduce compliance risks by improving the efficiency of the content review process.

As compliance team members conduct content reviews, the software tracks the progress of those reviews in an effort to identify any tasks that are falling behind. This review process is fully logged, thereby making it easy to prove to auditors that digital content has undergone a review process as required.

A review dashboard provides an overview of all review activities. This dashboard can help the organization to spot inefficiencies in the review process, while also drawing attention to overdue content reviews. There is even an alerting mechanism that can contact reviewers and compliance teams in the event that the review process becomes excessively backlogged.

By helping employees to work smarter, not harder, Proofpoint is able to streamline the compliance efforts of financial services companies. Proofpoint's software can help to greatly simplify your data archiving, eDiscovery, and review efforts.

Find out more: www.proofpoint.com

proofpoint.

Painterr / Shutterstock.com