The Bedrock of Financial Services: Trust

by Ryan Splain — October 13, 2021

Share on Facebook Share on Twitter Share on LinkedIn

Financial institutions are dependent on trust. Without it, people would not hand over their hard-earned money to banks and the entire global financial system would collapse. Regulations—while burdensome—exist to create public trust. However, complying with these regulations requires more than an earnest heart; it requires active accountability.

At its core, financial services compliance comes down to transparency: retaining records, reviewing non-compliant acts, and protecting user information. The only way to reliably have the data control to perform these actions is to have information governance as the foundation of compliance.

Removing blind spots

Just as the channels through which we communicate expand to new technologies, our compliance strategies must evolve as well. Regulations, like those stipulated by the SEC, FINRA, and SOX, cover all digital communications, requiring organizations to retain and supervise messages across email, social media, instant messages, and collaboration platforms. Manually managing disparate data sources independent of one another is an onerous task for compliance managers who are left juggling applications and platforms trying to catch messages before they hit the ground. Data governance eases the compliance process by virtually merging data sources together, allowing compliance managers to handle all communications as one.

Maintaining records

Accessing all data sources from a single platform alone is not sufficient if the platform cannot differentiate between records and non-records. Not every communication has to be retained, and not all retained communications have the same lifecycle. For example, protected records under FINRA and SEC preview must be kept in an immutable format for six years, whereas documents covered by SOX must be kept for seven years. While these are the largest regulators, there are numerous other legal mandates which have different definitions of what a ‘record’ is and how long they need to be retained.

Some financial services companies have “solved” their record retention problem by simply retaining everything forever. While this technically satisfies retention requirements, it is not sustainable in the long run. Not only will storing information in excess cost a premium as the number of digital communications continues to skyrocket, but it also poses a significant risk of data breaches as older records typically have outdated security settings and permissions.

To defensibly comply without retaining documents unnecessarily, organizations need to reliably classify their data in a host of categories so that each record can be given an appropriate lifecycle. Given the complexities in defining a record, a combination of metadata (time, place, owner, etc.) and content (the text of the communication, itself) is needed to assign policies. This deep understanding of communication data gives organizations the granular control to automatically place retention and deletion policies on data that satisfy all applicable regulatory requirements.

Monitoring compliance

While governance is helpful for retention, it is essential for supervision as it is unrealistic to monitor all enterprise communications for non-compliance. Organizations need some method to dwindle the number of documents for review, which requires a computational understanding of language. Most governance strategies rely on text indexing, which extracts all the words within a message and places them in a searchable ‘index.’ Rules can then be established to flag messages for review based on what each message contains. For example, any mention of keywords, such as fraud or guarantee, can trigger a review. Without this data control, reviewers would be incapable of ensuring that they are monitoring all non-compliant messages.

Adapting to the future

The need for governance is only set to accelerate as new regulations enter the fray. Notably, emerging privacy laws, such as GDPR and CCPA, expand the scope of protected data. These laws require organizations to be capable of finding, managing, and remediating sensitive information—wherever it resides.

The good news is that the same core technology needed to comply with financial services regulations can be leveraged to reach privacy by design. Just as supervision technologies can flag messages by keywords, privacy methods can isolate personal information, such as social security numbers, with pattern recognition software.

The primary challenge that financial services will face in the coming years is establishing governance not only in controlled, archived data but also in-place, at the source. Currently, organizations predominantly manage the sterile copies within the archive, leaving the original documents undisturbed. However, sensitive information can reside outside of the archive. Any attempt at privacy compliance that does not include in-place data will never be sufficient for full compliance. To meet these challenges, governance and compliance providers will have to expand their capabilities to encompass in-place data management.

Fin Serv compliance requirements exist for accountability, to ensure people’s trust in them is not misplaced. Data governance provides organizations the defensibility and control they need to account for their actions, account for their data, and maintain the trust in them required for global economic success.

Tags: compliance Customer privacy Financial Services Financial Transparency Industry Opinions Trust

Share on Facebook Share on Twitter Share on LinkedIn