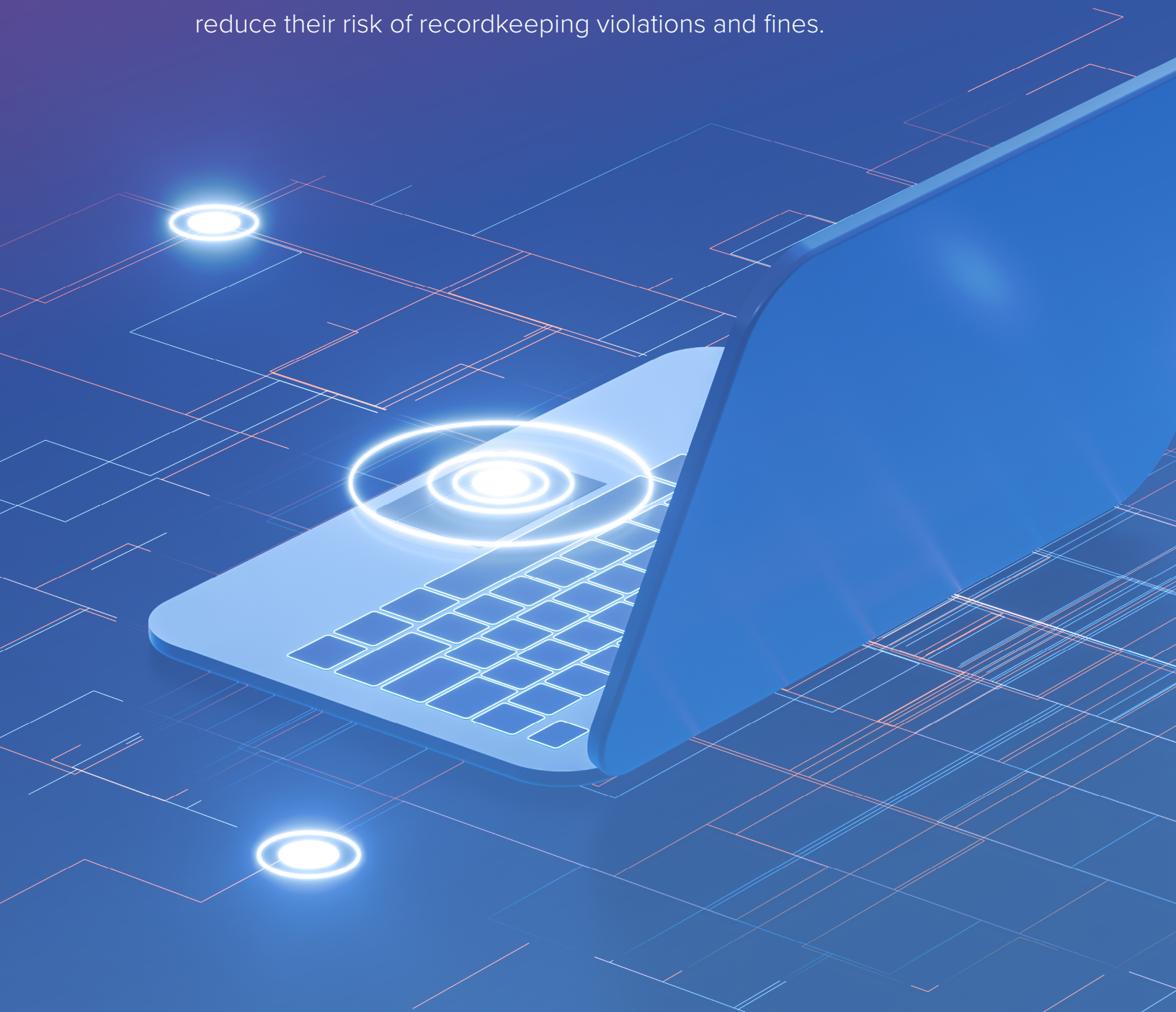
Electronic Communications Compliance Checklist

for Registered Investment Advisers

OVERVIEW

Registered Investment Advisers (RIAs) must maintain records of business-related electronic communications. But the requirements for electronic communications recordkeeping, storage and supervision can be daunting. However, with proper oversight, RIAs can help their business avoid the risks of litigation, fines or other enforcement penalties from the SEC.

This checklist outlines what all RIAs need to consider to reduce their risk of recordkeeping violations and fines.



Establish written supervisory procedures

SEC Rule 206(4)-7 requires firms to implement policies and procedures reasonably designed to prevent regulatory violations. Firms that have not already done so should adopt and periodically review formal written supervisory procedures (WSP).

When it comes to electronic communications, an effective WSP should establish:

- [ ] Standards for devices and applications that may be used
- [ ] Prohibition policies for devices and applications that may not be used
- [ ] Plans to monitor prohibited channels to catch off-channel communications
- [ ] Manual review processes
- [ ] Standards for digital ads or sales literature
- [ ] Guidance on sending confidential customer records or information

Know your records

Not too long ago, emails were the only electronic records RIAs had to capture and archive. Not anymore. Because of remote and hybrid office cultures as well as customer communication preferences, business conversations now travel seamlessly across workstations, mobile devices, apps and more.

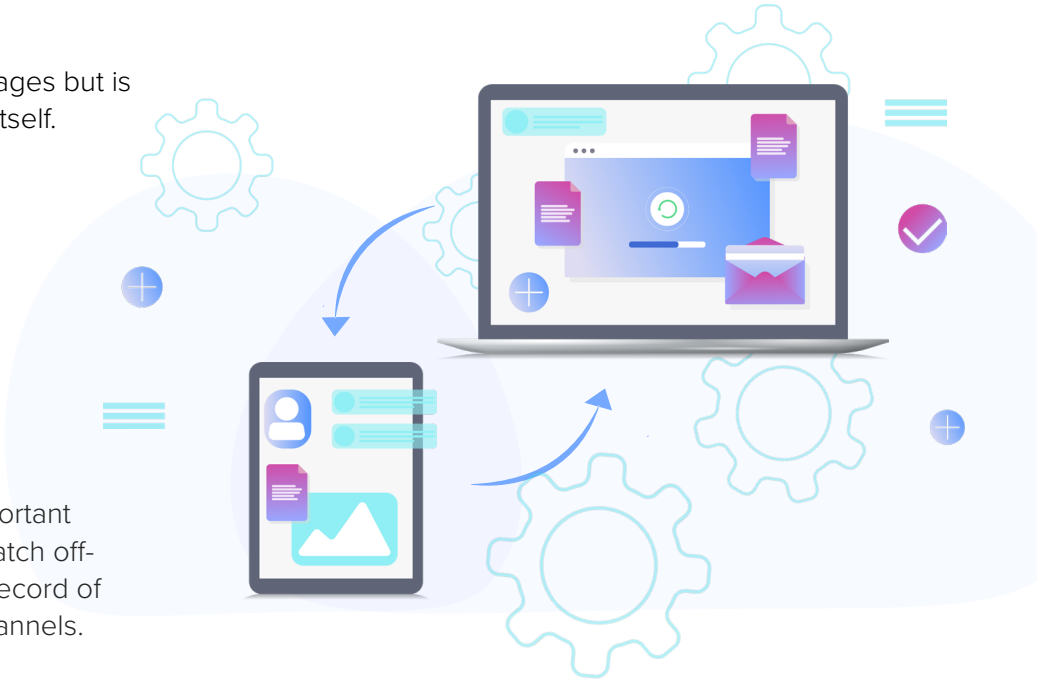
When creating a system for electronic communications compliance, ensure the system can capture all communications that are used for business and their associated metadata:

- [ ] Emails
- [ ] SMS/MMs text messages
- [ ] Instant messages
- [ ] File sharing
- [ ] Video calls
- [ ] Voice calls
- [ ] Social media posts
- [ ] Social media direct messages
- [ ] Social media comments
- [ ] Chatbot messages
- [ ] Encrypted messaging app communications (WhatsApp, WeChat)
- [ ] Collaboration app communications (Microsoft Teams, Zoom, Slack)

Metadata is data that is added to messages but is not part of the content of the message itself. This includes:

- Date and time sent or received
- Sender and receiver identification
- Message or conversation threading
- Attachments (including images) in messages

If a prohibition policy is in place, it's important to have a plan to monitor channels to catch off-channel communications, and to have record of the monitoring of those unapproved channels.



Storage system requirements

In accordance with SEC Rule 204-2, firms must retain books and records for five years from the end of the fiscal year during which the last entry was made. The first two years should be in the appropriate office of the investment advisor.

With the recent update to SEC Rule 17a-4, RIAs now have improved guidance and clarity on how to preserve and maintain accurate records. While there are multiple approaches to ensure compliance, the recordkeeping system must:

- [ ] Allow for independent access to records
- [ ] Have redundancy or back up records
- [ ] Be able to accurately produce or reproduce records of any particular time period
- [ ] Be able to download and transfer copies of records on both human readable format and in an electronic format that's compatible with commonly used systems
- [ ] Have an audit system in place
- [ ] Reasonably safeguard records from loss, alteration or destruction

SEC 17a-4 now allows RIA firms to use an audit trail to satisfy recordkeeping requirements as an alternative to traditional WORM storage.

Firms that preserve required records electronically using a "third party" must file a Third-Party Access Undertaking or update current filing with their Designated Examining Authority (DEA).

Supervision requirements

Simply capturing and archiving records isn't enough. SEC Rule 206(4)-7 requires firms to establish, maintain and enforce written policies and procedures to detect and prevent compliance violations, including the misuse of non-public material information.

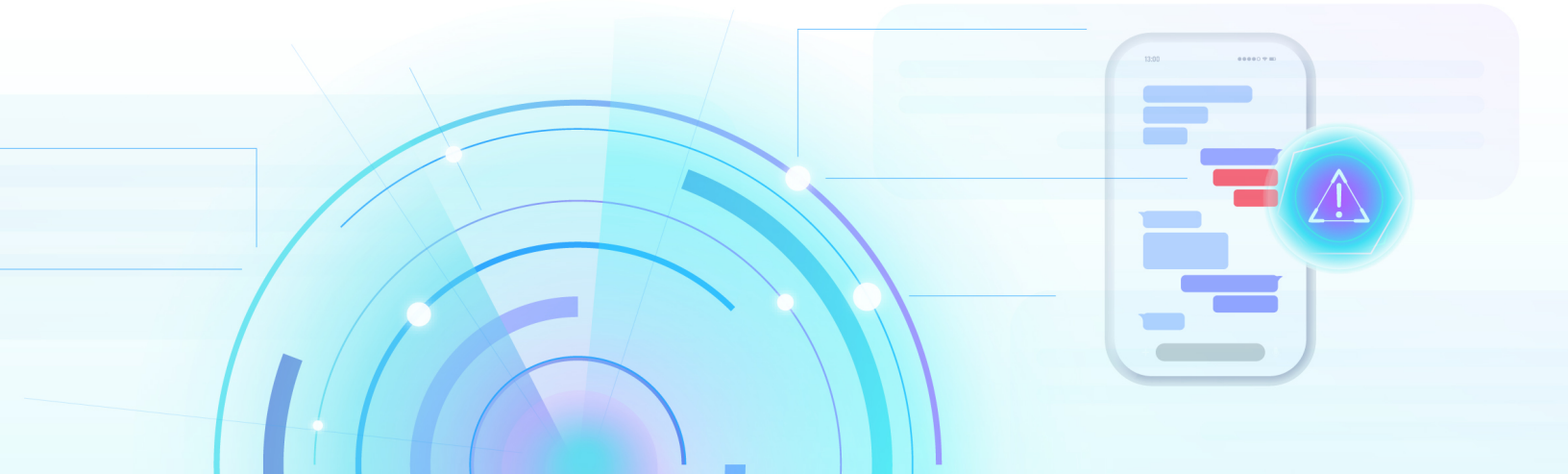
This requires a system that can arrange and index records in a way that permits:

- [ ] Fast and accurate searches
- [ ] Easy and reliable retrieval of records
- [ ] Search and retrieval of records of specific time periods

As communication data volumes increase in size and variety, it's important for RIAs to have recordkeeping solutions that can support their compliance teams.

This means having a system that can identify and flag the following for additional review:

- [ ] Phrases such as "text me," "send to my personal email," "direct message me on LinkedIn," etc. (lexicons can be created to identify such phrases)
- [ ] Potential regulation best interest (Reg BI) violations
- [ ] Communications sent to/from an employee's personal (non-work) email or indications of other off-channel communications
- [ ] Conflicts of interest (gifts and entertainment, political contributions)
- [ ] Communications from individuals considered "high risk"
- [ ] Client complaints
- [ ] Guarantees of performance
- [ ] Outside business activities (OBA)
- [ ] Client information/personal information sent unencrypted/not secured



Mobile supervision

Businesses are becoming increasingly reliant on mobile devices and apps. As long as the communication is business-related, all messages that are sent or received on mobile devices must be archived and supervised.

Firms need to identify what channels employees are allowed to use and then make sure they're capturing and preserving that content. Equally important, firms need to have a plan in place to ensure prohibited channels aren't actually being used.

Every firm that permits its employees to communicate, with regards to its business, through text messaging apps or chat services must first ensure that it can retain records of those communications as required by SEC Rule 204-2. Introducing new devices into the corporate ecosystem requires careful consideration of device scenarios, which types of devices are allowed, operating systems and wireless service providers. These questions will help you define device policies and simplify the management of proper deployment.

If a firm allows the use of mobile devices to send and receive business communications, they must be prepared to capture these communications. This applies to firm-provided devices or an employee's personal device if the firm has a bring-your-own-device (BYOD) policy:

- [ ] Emails
- [ ] Text messages
- [ ] Social media posts
- [ ] Social media direct messages
- [ ] Messaging on collaborative platforms like Zoom, Skype and Microsoft Teams
- [ ] Messages on encrypted apps like WhatsApp and WeChat

Need help checking items off this list?

Regulators have made it clear that there will be no debate when it comes to recordkeeping and supervision — even as communications technologies continue to evolve and grow increasingly complex.

Smarsh simplifies compliance by automating communications capture and supervision workflows. Our software and services are purpose-built to meet compliance obligations (FINRA, SEC, NIST, GDPR and more), so RIA firms have the tools they need for success.

Smarsh empowers firms' compliance teams to cost-effectively stay on top of regulatory requirements.

Visit www.smarsh.com to learn more.

This checklist is not intended to be exhaustive and does not fully account for differences among regulatory bodies of the securities industry in non-U.S. markets. Compliance professionals should visit SEC.gov for a complete analysis of applicable rules and regulatory guidance.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Checklist - 03/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh