charles SCHWAB

Advisor Services

Compliance Review

Ongoing compliance updates for independent advisors

December 2018

IN THIS ISSUE

I. Introduction . . . 1
II. Assessing the regulatory landscape . . . 2
III. Understanding the key components . . . 3
IV. General operations: Best practices . . . 6
V. Storage: Best practices . . . 9
VI. Conclusion . . . 12

Books and records: Key definitions and considerations for investment advisors

Patrick J. Burns, Jr., JD, President and Co-founder, Advanced Regulatory Compliance, Inc.; Managing Attorney, Law Offices of Patrick J. Burns, Jr., PC

Diana Chen, Compliance Consultant, Advanced Regulatory Compliance, Inc.; Senior Transition Coordinator, Law Offices of Patrick J. Burns, Jr., PC

Damian Lo Basso, Founder and CEO, Compass CFO Solutions, LLC

I. Introduction

Sprung from a report made by the Securities and Exchange Commission ("SEC") to Congress over the previous decade regarding the Public Utility Holding Company Act of 1935 ("PUHCA"),[1] the Investment Advisers Act of 1940 ("Advisers Act"), like the PUHCA, sought to protect the interests of ordinary consumers.[2] More significantly, the Advisers Act formed guidelines for the unique fiduciary duty advisors have to their clients, seeking to eliminate, or at least expose, conscious or subconscious conflicts of interest on the part of advisors. The Advisers Act consists of a set of recordkeeping requirements that regulate the performance of advisory firms as both businesses and fiduciaries. Records should be kept under the Advisers Act as evidence of fiduciary duty, and advisors should be able to refer to the Advisers Act for best practices that can ensure diligent recordkeeping and organization from an operational perspective.

Historically, the SEC has enacted a "broken windows" policy toward books and records enforcement. Though it has modified its mentality that it is beneficial to go after advisors guilty of minor infractions to prevent larger transgressions, the overall premise is not entirely flawed. If an advisor's foundation is not solid, the chances of successfully building on that foundation remain slim. Properly understanding the role that maintaining accurate books and records plays in a successful firm, displaying diligence in instituting policies and procedures to maintain compliance, and leveraging the end result to best position the firm are key to building a foundation set for success.

This white paper will not only address the recordkeeping responsibilities of investment advisory firms from operational and fiduciary perspectives but also outline best practices for the maintenance of books and records.

[1] Staff of the Investment Adviser Regulation Office, Division of Investment Management, U.S. Securities and Exchange Commission, *Regulation of Investment Advisers by the U.S. Securities and Exchange Commission* (2013).

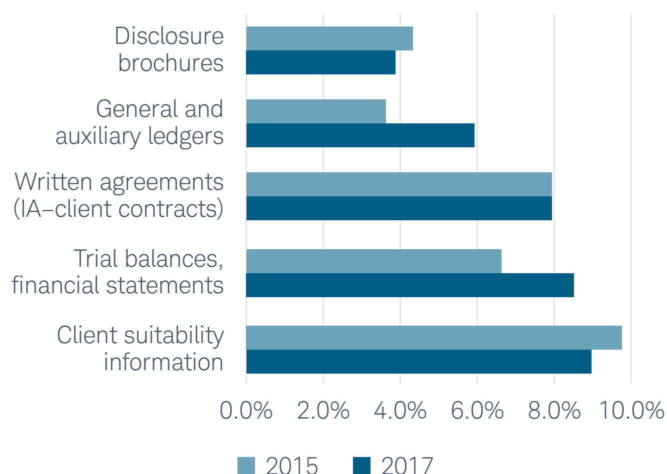
[2] Scott C. James, "Progressive Republicans and the 'Death Sentence' for Public Utility Holding Companies During America's Second New Deal," in *Presidents, Parties, and the State: A Party System Perspective on Democratic Regulatory Choice, 1884-1936* (2000; repr., New York: Cambridge University Press, 2006), 228.

II. Assessing the regulatory landscape

Overview

While the SEC does not require firms to include specific elements in their books and records policies and procedures, firms are expected to properly analyze their operations for compliance obligations and develop controls to mitigate the risks associated with such conflicts.[3] At the onset of an examination, an advisor's response to records requests often provides regulators with an initial impression of a firm's internal controls. Regulators can easily sanction advisors for failure to maintain proper records, even when the rest of an examination reveals no additional deficiencies. According to the North American Securities Administrators Association, of the 1,227 state examinations conducted on investment advisors in 2017, 64.6% found books and records deficiencies.

Investment advisors' top five books and records deficiencies



Source: North American Securities Administrators Association, Investment Adviser Coordinated Exams (released Q1 2018 and Q1 2016).

Understanding deficiency penalties

When considering the penalties and sanctions that can be imposed on an advisor, either through the court system or via the SEC, the scope of a judgment is based on "each act or omission." This standard, however, can be interpreted in multiple ways. Take the case of an advisory firm that distributes inaccurate fund performance information to 10 potential investors. One ruling may find that each of the 10 investors who received inaccurate information constitutes a separate violation, while a second might rule that the distribution of inaccurate performance constitutes a single violation.[4] In either event, in January 2018, the SEC updated the maximum civil money penalty for each act or omission violating the securities laws (see table below).

While severe, the mentality behind the large penalties is to help eliminate any arbitrage opportunities, where advisors ultimately determine that any monetary fines they may face will be lower than the cost of hiring the proper support to remain compliant.

Proactive preparation

Maintaining proper policies and procedures is often the first way of ensuring a firm is fully prepared and compliant. Even before they receive a notice of examination, advisors can prepare well in advance for a documentation request.

Inflation adjustments to the civil monetary penalties administered by the SEC (as of January 15, 2018)

		Individual		Entity	
		2015	**2018**	**2015**	**2018**
Tier 1	Any violation	$7,500	$9,239	$80,000	$92,383
Tier 2	A violation involving fraud, deceit, manipulation, or deliberate or reckless disregard of regulatory requirement	$80,000	$92,383	$400,000	$461,916
Tier 3	A violation that also involves a substantial risk of loss to others or gain to the violator	$160,000	$184,767	$775,000	$923,831

Source: "Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission," U.S. Securities and Exchange Commission, January 15, 2018.

[3] U.S. Securities and Exchange Commission, "Information for Newly-Registered Investment Advisors," last modified November 23, 2010.

[4] Reference based on examples provided by Jonathan N. Eisenbert in "Calculating SEC Civil Money Penalties," Harvard Law School Forum on Corporate Governance and Financial Regulation, January 24, 2016.

Maintaining a system that tracks the locations, retention period, method of storage, and responsible party is a simple way to begin implementing proper policies. Note that the responsible party should not only maintain all relevant documents but also destroy all records after the applicable time period has passed. Keep in mind that regulators are entitled to review maintained documents, even those held longer than the required period.

The advisors who fare best during document examinations realize that preparing the firm for them is an ongoing task. These firms provide written guidance, to be reviewed annually by all employees, that outlines firm policies on identifying compliance risks and describes the process for implementing new procedures to mitigate those risks. Proper training is imperative to ensure that policies are followed and to reinforce the importance of being diligent during normal business tasks.

Note that the responsible party should not only maintain all relevant documents but also destroy all records after the applicable time period has passed. Keep in mind that regulators are entitled to review maintained documents, even those held longer than the required period.

III. Understanding the key components

Determining which books and records should be kept and how can be a leviathan task. This endeavor, however, can be simplified by thinking of an advisory firm as an entity that interacts with its surroundings. These interactions are composed of three main components: an action component encompassing advisory activities; a product component for items offered, such as marketing materials and model portfolios, that are unique to the firm; and a functional internal component. As such, we can divide the books and records to be kept for an advisory firm into these three categories.

Action and power items

When thinking about compliance in the investment advisory business, the key phrase is *fiduciary duty*. This phrase is particularly important when it comes to the client-facing services that representatives provide. For advisors to successfully provide advice to a client, the client must grant them the necessary privileges to do so, and for the advisors to continue providing advice, additional records of their activities will need to be kept and/or updated. To an examiner, these records are the best depiction of fiduciary duty being conducted. Therefore, we may rephrase the previous statement to assert that in the eyes of examiners, books and records are to be kept by advisors in order to secure the right to service their clients.

Disclosure

Advisory agreements and Form ADV, Parts 2A and 2B firm and advisor disclosure documents are basic items that establish an advisor's right to perform advisory services. In addition to signing advisory agreements, clients must also be provided sufficient disclosure, via Form ADV, Parts 2A and 2B, of the services they are entering into, who is providing them, and their providers' possible conflicts of interest. This disclosure and affirmation structure is something we will see again when discussing electronic signatures.

Generally, any items that could influence the client's experience with your firm would warrant a disclosure in the Form ADV, Part 2. This would include direct conflicts of interest, such as fee-sharing arrangements with third-party firms, and indirect items that may affect the client's interaction with your firm as a whole. For instance, arrangements with other companies to market to your clients in any way would likely warrant disclosure. A conservative approach is also advised when it comes to affirmation. Any material changes to the service a firm provides a client should result in that client being notified at least and being repapered at best.

Suitability

Inherently, more complex services require firms to have more privileges and therefore more affirmations from clients. Oftentimes, simple disclosure does not suffice. Firms will be expected to provide documentation of fiduciary duty being done and of their capacity to fulfill fiduciary standards in situations where special rights are given to advisors, such as custody. Therefore, when it comes to records related to advisors' ongoing actions to service their clients, the key word is *suitability*.

On the primary level, ongoing documentation must be kept that depicts services taking place as promised. For instance, when creating a financial plan for a client, the advisor must correspond with the client and keep records of the plan being formed. For asset management, this means that trade blotters and memoranda and all relevant client account records, including but not limited to account-opening paperwork, power of attorney, beneficiary and trustee designations, and information regarding tax status, must be kept. While the bulk of current client information can

be accessed on custodial platforms, the length of time that such data will be preserved is not guaranteed, and advisors should consider pulling client records annually to ensure they are not lost.[5]

"Memoranda" include all relevant details of an order, including its terms and conditions, instructions, modification or cancellation, the broker-dealer through which it was executed, and so on. Most often, deficiencies in tickets and memoranda occur when firms fail to disclose who recommended the transaction, who placed the order, and whether discretionary authority was used to execute the trade. To prevent these deficiencies, firms may take a risk management perspective: The trade recommender should be licensed and cannot also serve as the order placer, because this could create a conflict of interest, and nondiscretionary authority should be indicated at appropriate times to limit liability, especially if a firm routinely exercises discretionary authority.

Conversations with clients must also be documented; summaries of conversations may be stored on client relationship management systems. Documentation that confirms that a service is being performed as promised often must—and always should—be kept and is particularly useful in cases in which higher-than-normal fees are charged; examiners will rely on these records to evaluate whether fees are justified.

On the secondary level, as a best practice, firms may conduct written reviews annually to ensure that services provided to clients are suitable. The examiner assigned to a firm during an audit will ultimately decide how often suitability reviews, and documentation thereof, should be conducted, and this can range from annually to once every three years. The more iterations of management services a firm offers (discretionary vs. nondiscretionary, wrap vs. non-wrap, broker-dealer vs. advisory account), the more factors must be reviewed to justify keeping each client in one account type versus another. Written reviews do not need to be extensive but should contain enough information to capture changes in a client's investment objectives and the firm's justification for maintaining or changing the client's account type. Usually, custodial platforms require clients to update suitability forms once a year, making it best for firms to pull these forms annually.

Custody

Furthermore, firms must be aware of the broad range of activities that count as custody. Essentially, whenever a firm may make deductions from a client's account or otherwise has access to a client's funds without an intermediary (such as a custodian or bank), custody is likely triggered. But not all custody is equal. Some forms of custody may warrant more reporting requirements than others.

For instance, custody is triggered when a firm deducts advisory fees directly from accounts under management. However, as long as state-registered firms and their custodians both send invoices to their clients, disclosures need to be made only in the Form ADV, Parts 1 and 2A, and assets under management for accounts custodied this way do not need to be reported.

Custody may also be triggered when firms use clients' standing letters of authorization for third-party disbursements. In this case, custodied assets under management should be documented, but an annual surprise examination may be avoided if a certain set of conditions are met.

When custody is clearly triggered—for example, when an advisor acts as trustee to a client's account—advisory firms must meet further requirements to prove they are financially apt to take on the responsibility. SEC- and state-registered firms are subject to annual surprise exams of accounts under custody and must hire a qualified accountant to conduct these. Balance sheets must be prepared according to generally accepted accounting principles ("GAAP"), and assets under management must be updated at least once a year during a firm's annual amendment. While amounts vary by state, most states also require state-registered firms to submit balance sheets annually to their department of business oversight that depict a minimum net worth. Responsibility rests on the firm to submit these materials. Unfortunately, states do not always reach out in a timely manner. Advisors, therefore, may do well to look up their state's minimum financials submission requirements.[6] Meanwhile, SEC-registered firms must only maintain a positive net worth and are subject to no additional filing requirements.

Learn more about the Custody Rule and its implications

To learn more about custody and its implications, we suggest reading Schwab's Compliance Review from May 2017, *Custody: New SEC Guidance Creates More Clarity*. You may also visit the Custody Rule Service Guide page on schwabadvisorcenter.com for additional tools and resources.

Materials-related items

Firms may also create their own materials and products, such as advertisements, websites, performance reports, or model portfolios. Adopting a product perspective, whereby a firm regards each proprietary item it uses or distributes as an independent product, is helpful in ensuring that the firm

[5] From a regulatory perspective, custodians must adhere to the five-year rule pursuant to the Advisers Act. However, there is no guarantee that records will be easily accessible for all five years or that custodians will ultimately adhere to these rules. 17 C.F.R. § 275.204-2 (2016).

[6] This is not always a full balance sheet. In California, for example, a simple minimum financial requirements worksheet must be filled out and submitted with a signed verification form. The numbers will then be confirmed during an audit.

captures its recordkeeping responsibilities. For these items, states generally follow the lead of the SEC.

Advertisements, websites, and social media

Products are often improved, and each improved product is distinct from its previous version. Take a webpage, for example. If an updated webpage provides a function that the older page did not, it will be considered distinct from its previous version, and both versions must be recorded. Because the main function of your firm's website is to provide information on the firm and its services, adding new qualitative information to the page or changing clients' access to the information—such as when a page is reformatted—would constitute updates. Conversely, if qualitative information is removed—for example, when an advisory firm ends its affiliation with a broker-dealer—an update must be recorded. When archiving, therefore, the best solution is to find software that archives *per update* instead of per unit of time. A variety of website creation and archiving platforms are available. The advantage of higher-tech solutions, compared with traditional copy and save strategies, is that small but significant changes to a page, such as additions to a drop-down menu, may be captured in a lot less time.

Advisors must also keep in mind that fiduciary duty should be tied in to the materials they create and provide to clients. As firm websites are informative in nature, providing adequate disclosures prevents misinterpretation and ensures that information on such sites is delivered in a true and accurate manner. Sources of information should be referenced and cited if they are not general knowledge—meaning easily confirmable by the average person. For less accessible sources, such as research reports or journal articles that require subscriptions to view, it is best practice to keep a copy of the document on hand or at least be able to access it upon request, perhaps through a subscription. For performance reports, the same applies, but to a greater extent. As of 2016, the SEC has tightened its recordkeeping requirements for firms distributing performance reports. Direct and indirect communications to any single person that include performance claims must be maintained for five years. Furthermore, advisors must maintain originals of all written communications received and copies of written communications sent relating to the performance or rate of return of any managed accounts or securities recommendations.[7]

Proprietary products

So far, we have not touched upon model portfolios. When assessing what documentation to keep on record, keep these questions in mind: *Is the model an appropriate tool for the client it was assigned to? Will the model be useful in the future?*

For the first question, consider this example: A firm is implementing the model portfolios of a third party. Fiduciary duty is shared between the two parties, but the scope of duty relies on the role each party plays in the formation and implementation of the models. As the implementer of third-party model portfolios, an advisory firm must show that it has chosen a suitable model for its clients' needs. To do so, the firm will maintain documentation of all due diligence completed in selecting the model portfolio and match it to each client, and it will provide a sufficient description of how the model portfolio was created. While the model creator is ultimately responsible for maintaining the research and analysis conducted in forming the model, a best practice for firms is to maintain details sufficient to show enough was known about the model to properly assess suitability; clients may also be given an informational brochure to ensure that they understand the model portfolio they were assigned. Transparency is key when answering *why*. Performance reports, for instance, should be backed by documentation supporting why specific benchmarks were chosen to compare returns against. Because it is often difficult to find perfect benchmarks, examiners greatly appreciate transparency.

Our second question—*Will the model be useful in the future?*—is relevant, considering records must be kept for five years after they are last referenced. It is prudent for firms to hold on to records of old materials for more than five years if they plan to improve upon them, such as with proprietary strategies, or cite them in future materials, such as past awards.

Targeted audiences

Firms should consider whether a product was targeted toward a specific group. As a rule, any time a firm targets an exclusive audience, it should keep a record of the recipients. According to the Advisers Act, recipients' names and addresses must be kept when a notice, circular, letter, or announcement is distributed to 10 or fewer people. Note that "distribution" encompasses instances in which a group is enabled, such as through the use of a password, to access certain marketing materials. Additionally, for all distributions, if a specific list is used to target recipients, a record describing the list and its source must be kept.

Structure items

The third and final set of records to be maintained is related to an advisory firm's form and function, corporate structure, and internal and external operations. This set comprises articles, agreements, and policies. Again, the overarching theme is that these records are relevant and accurate to the actual setup of a firm and the policies it implements.

[7] 17 C.F.R. § 275.204-2 (2016).

Internal policies and day-to-day functions

There is a key set of compliance documents every firm should have: written supervisory procedures ("WSPs"), a business continuity plan ("BCP"), a privacy policy, a code of ethics, a cybersecurity policy, an organizational chart, and, if SEC-registered, an identity theft protection policy. Most internal documents, such as the BCP, code of ethics, and cybersecurity policy, may be included in a firm's WSPs. Essentially, the WSPs provide sufficient answers to a firm's "what if's": *What if there is a cybersecurity breach? What if an investment advisory representative trades ahead of a client—is there a personal trading approval process in place to prevent this? What if there is a significant business disruption?* Above all, internal documents accurately describe the steps firms take to ensure smooth and ethical operations.

Cybersecurity policies help ensure clients' personal information is protected, while privacy policies let clients know how their data is being used. When it comes to both, advisors may think of their firm not as a static entity, but as a team consisting of members constantly interacting with other internal and external entities. Therefore, fiduciary duty for cybersecurity should extend to all third parties that have access to client information, such as IT companies and independent contractors. In fact, it is crucial that SEC-registered firms have a strong cybersecurity policy in place that is tailored to the specific needs of the functions they perform and that ensures vendors are reviewed and selected with due diligence.[8] To prevent vendor failure, which has been responsible for some of the largest data breaches in past years, firms may hire independent companies to perform penetration tests on their vendors. Finally, firms of all sizes must report cybersecurity incidents in a timely manner. As a best practice, a log should be kept of the incidents that occurred and the steps taken to resolve them and prevent them from occurring again.

Privacy policies, on the other hand, inform clients of all the ways their personally identifiable information (i.e., information from which their identity may be deduced) is used and shared, with a focus on information sharing that is outside of what is required for advisory services to take place. In the United States, clients must be given the option to opt out of allowing their personal information to be used or shared for purposes that are not directly related to the advisory service(s) being provided to them. For instance, clients must be given the option to opt out of receiving marketing materials. In the European Economic Area, where the General Data Protection Regulation regulates the transfer of data, clients must opt in to provide information for these ancillary functions.

Policies for external functions

External policies relate to a firm's relationships with affiliates and outside parties. An examiner may request records that indicate any relationship that may affect a client's investments, such as those for initial public offerings in which members of a firm participated, agreements establishing control relationships, proprietary accounts, and interest in private equity. To be conservative, firms may consider keeping records of any relationship or action that significantly changes its status in the financial landscape.

Similar to those for cybersecurity, best practices here involve accounting not only for an advisory firm but also for all its extensions. For instance, employees become extensions of a firm when they use its resources and rights (as investment advisors registered at the firm) to perform services. Therefore, if an advisor enters any setup that may be a conflict of interest, it must be disclosed. The degree of disclosure and associated documentation that must be retained is generally determined by the amount of authority, direct or indirect, that an advisor has in the outside venture and the effect it may have on clients. For instance, private equity, which is reserved for accredited investors, bestows a lot of influence—and therefore fiduciary duty—on the advisor(s) managing or invested in it. If advisors, as extensions of a firm, are engaged in a private equity venture, the firm should also be considered as taking part. Thus, the proper documents to ensure proper operation of this extension of the firm—such as organizational charts, brokerage agreements, custodial information, and offering memoranda—should be kept on file.

IV. General operations: Best practices

When implementing the proper policies and procedures to adequately meet books and records compliance obligations, a firm must make several decisions to best position itself and its partners for success. Advisors who do not have access to trained personnel to properly manage their financial books and records have a stronger need to understand the resources available to manage these requirements. Fortunately, advancements in technology have helped create a seamless work flow that provides advisors with the tools to help them remain compliant while operating in an environment that maintains the highest level of security to protect against the most common threats.

Historically, advisors relied on locally maintained software, often accessible from a single terminal, and multiple individuals used the same credentials. Manipulation and integrity risks notwithstanding, instances in which financial statements maintained on a local hard drive became corrupt prior to being securely backed up would immediately move an advisor out of compliance should an auditor ask the advisor to produce those statements.[9]

Fortunately, the past decade has given rise to sophisticated and secure cloud-based solutions that help eliminate the key risks advisors face with locally hosted solutions. A

[8] Office of Compliance Inspections and Examinations ("OCIE"), "OCIE's 2015 Cybersecurity Examination Initiative," *National Exam Program Risk Alert*, IV, no. 8 (September 15, 2015).

[9] 17 C.F.R. § 275.204-2 (2016)—Books and records to be maintained by investment advisors.

Key factors to consider when evaluating tools to handle sensitive firm and client information

Key factor	Meaning	Criteria
Authentication	How does the technology validate your identity to prevent unauthorized access?	Uses multifactor authentication, CAPTCHA, or physical token strategies
Access control	Can you control who has access to the information (e.g., employees, contractors, etc.)?	Multiple login capabilities, user control functions, audit trails
Data security (encryption)	How does the technology protect your data?	Transport Layer Security (TLS), Data Encryption Standard (DES), Twofish, RSA
Protective technology	What steps are taken to protect the data centers hosting the technology?	Physical security, power and cooling backups, data redundancies
Security monitoring	Is the technology actively monitoring for threats?	Active monitoring for unauthorized intrusions and access, file changes, and unplanned spikes in activity
Business continuity and disaster recovery	What steps are in place should an individual data center go down?	Active replication of data across multiple data centers (in different geographic regions), regular system backups, multiple systems providers

variety of technology platforms offering accounting solutions for advisors adhere to the highest levels of security, providing advisors with unrestricted access to their firm's information and a secure work environment in which to operate. Part of an advisor's job is dealing in confidential client information, and the handling and transmission of that information requires an advisor's, and his or her team's, highest consideration. When evaluating tools to handle sensitive firm and client information, advisors can consider the table above.

Items unique to transitioning advisors: New launches and tuck-ins

While all advisors operate under the same regulatory oversight, issues facing transitioning advisors require additional diligence. Understanding the nuances of these unique circumstances is paramount to avoiding regulatory scrutiny, even before a firm is formally registered. One of the most highly scrutinized activities that a transitioning firm must properly document and disclose is the receipt of transition support funds from its chosen custodian. Transitioning advisors are commonly offered custodial support funds to assist in converting existing clients to a new custodian. These funds are typically released to cover certain eligible expenses once predetermined conditions are met. Eligible expenses include marketing, technology, and certain consulting and research activities. To comply with the Advisers Act, advisors who receive these support funds must disclose to their clients and prospective clients the terms of the arrangement and any conflicts that may arise because of it. Records of all funds received and remittances to approved vendors, as well as evidence of proper disclosures, must be maintained by the advisor in accordance with all applicable rules and regulations.

A simple rule of thumb when figuring out whether custodial support funds can be used to pay for an expense is to determine whether that expense will continue to have inherent value after the transition is final. For example, marketing services to launch a firm are eligible, whereas computers, furniture, and other hard assets are excluded.

Additionally, transitioning advisors need to maintain and document any out-of-pocket expenses they incur before the formal launch of their firm. In most instances, advisors incur costs for legal services, office furnishings, and technology buildouts that are directly related to the launch. Advisors are encouraged to keep detailed records of all out-of-pocket expenses, and not just to remain compliant with applicable regulatory bodies. Proper documentation is required to record an advisor's capital position in the firm. Most launch-related expenses incurred by an advisor are eligible for beneficial tax treatment when the advisor decides to take a distribution, though the IRS requires that proper records be maintained for verification.

While advisors in transition need to be aware of a unique set of protocols and requirements, firms that are acquiring or looking to acquire advisors with preexisting books of business also have their own list of best practices to maintain. With the demand to buy existing books of business greatly outpacing the supply, firms properly suited for scale gain a significant competitive advantage in the market. The initial diligence process offers acquisition targets their first glimpse into the internal operations of an acquiring firm. The ability of a firm to quickly produce its internal policies and procedures—on items such as payout structure, corporate expense protocols, and financial reporting metrics, among others—reflects the institutional framework many sellers desire.

One of the primary drivers for advisors looking to "tuck-in" to an existing firm is the ability to bypass many of the operational hurdles of launching a brand-new firm. The economics surrounding a transition are always critical, but oftentimes advisors will look to join an existing firm to accelerate their ability to scale and to significantly increase their operational efficiencies. By adhering to operational best practices, a firm not only saves new advisors from having to re-create the wheel but also significantly reduces the time it takes to integrate new advisors into a firm's culture, technology, and vision.

Audited vs. reviewed vs. compiled financial statements[10]

If, after careful review, advisors want to proactively seek the opinion of an independent third party to attest to the accuracy of their controls and financial statements, they can choose from several options. Each option must be performed by an independent CPA in accordance with GAAP.

An audit gives a firm the highest level of assurance that its financial statements are in good order, ensuring that they are free of material misstatements and are fairly presented in accordance with GAAP. Auditors can determine this by communicating and verifying information with outside parties, testing selected transactions by examining supporting documents, completing physical inspections, and thoroughly evaluating a firm's internal controls. Though typically much higher than the cost of a review, the cost of an audit depends on the complexity of the firm and the scope of the engagement.

If a firm does not want to pay for a full audit or feels that an audit is not warranted, it can hire a CPA to perform a review of its financials. While not as thorough as a full audit, reviews, which involve limited inquiries and analytical procedures, can reasonably assure firms that their financial statements are free of material misstatements and comply with GAAP.

If a firm does not need to be assured of the accuracy of its financial statements, it can have a compilation performed, whereby a CPA will use information provided by the firm to create financial statements that comply with GAAP. No testing is performed to ensure that the information provided is correct or free of material misstatements.

Financial books and records resources

To the average advisor, maintaining accurate financial statements, complete with all support and documentation, is a daunting task. Maintaining proper financial controls regularly falls to the bottom of an advisor's priority list, whether due to a lack of staff or a lack of institutional knowledge. Fortunately, advisors who have decided that their firm's resources are better spent on revenue-generating tasks can still find support.

Typically reserved for larger firms, hiring in-house personnel in the form of a chief financial officer, controller, or bookkeeper is the most obvious way to gain the support needed to meet financial and accounting obligations. While the benefit of having an on-site employee to address

Looking for more information on compliance or regulatory issues?

Schwab's compliance website includes a searchable database, compliance tools, and many other resources to assist you. Visit schwabadvisorcenter.com > News & Resources > Compliance. (See "Online compliance resources" on page 12 for more information.)

[10] American Institute of CPAs, *Guide to Financial Statement Services: Compilation, Review and Audit*, 2015.

issues in real time is a nonnegotiable luxury for some, there are often overlooked costs associated with these hires. And when you consider an employee's salary, benefits, technology, and other ancillary expenses, that cost is often two or three times more than that of other solutions.

For firms that cannot afford on-site employees, leveraging the services of a third-party CPA firm can be attractive. Most firms will limit the engagement to financial statement preparation and tax services, and the cost of implementation is often a fraction of the cost of a full-time hire. CPA firms specialize in and often guarantee the completeness and accuracy of an advisor's financial statements. That said, they are typically not equipped to perform the other operational and administrative functions required to properly manage a firm's accounting and finance departments.

Advisors seeking timely and accurate financial statements at a reasonable cost and operational support for their staff often utilize boutique consulting firms that specialize in working with independent financial advisors. These firms, which often have a cost structure like that of traditional CPA firms, have experience dealing with the issues commonly faced by advisors and their staff. Their experience typically extends beyond traditional bookkeeping and tax work and includes financial modeling and budgeting, back-office operational support, and internal controls.

V. Storage: Best practices

Keep books and records for five years, domestically, with the first two in office. Separately store duplicates of these records for five years as well. And make sure all records are easily accessible and retrievable. A firm that follows these directions has fulfilled its retention obligations pursuant to Rule 204-2 under the Advisers Act.

Easily retrievable vs. easily accessible

It is necessary to define these terms and their distinction. In this section, "retrievability" refers to how easily a record can be found, while "accessibility" refers to how easily a record may be interacted with (viewed, reviewed, saved, and so forth). "Retrievable" corresponds with knowing where a record is stored, while "accessible" corresponds with obtaining a copy of a record of interest.

Firms should consider making a habit of adding a basket of new documents to their records annually, alongside annual best-practice reviews of items such as their WSPs, cybersecurity policy, BCP, and required updates of their Form ADV, Part 2. Firms can date and organize all versions of documents in folders for easy retrieval. Because books and records storage requirements are relatively straightforward, we will dissect only a few gray areas of recordkeeping in this section.

The first is the duplicates requirement, which ensures that copies of all originals can be retrieved if they are lost. In general, an appropriate storage medium for a duplicate is easy to access and retrieve from, and it clearly depicts the complete original. Advisory firms commonly use backup and archiving services to meet this requirement. Both archiving records and backing up records have their advantages and drawbacks, and the best policies use them together.

Backups serve to restore lost data and therefore allow operations to progress quickly after an incident. They do a good job of meeting the "easily retrievable" requirement when time is of the essence, but they might not be "easily accessible." Because their purpose is to allow business to progress, backups might not be saved in perpetuity; each restoration may recover only data backed up after a certain point. On top of this, backup technologies often store data in a way that minimizes space, making data difficult to search. If an original document is permanently deleted, backups may also be difficult to retrieve. Supplemental practices, such as routinely saving backups on a hard drive or maintaining a secondary server, may be implemented to reduce the drawbacks of backups if archiving software is not used. When determining how often to perform retrieval tests, firms should determine how much information stored on each backup device they can tolerate to lose and test according to the durations of time that correspond with this loss. Similarly, test restores should be done regularly for books and records backed up by cloud software. Firms should also conduct tests following software updates because new versions of software could cause backup failures.

The best way to compensate for the limitations of backups is to utilize archives as well. Archives maintain historical data for long periods of time, including in perpetuity, and are stored independently of originals. Think of an archive as a copy rather than as a mirror image. Therefore, if an original document is deleted, the archived copy is not affected. Most significantly, unlike backups, many archives are easily searchable. They may analyze, classify, and sort data into a format that is user friendly. For records that require review, such as emails for which due diligence must be conducted for material information and promissory language, archiving offers a full solution, while backing up does not.

By the Advisers Act, electronic media may be used to store original books and records. With the prevalence of eSignatures and online storage systems, it is no surprise that electronic records are replacing paper ones.

Electronic records

The passing of the U.S. Electronic Signatures in Global and National Commerce Act ("ESIGN") in 2000 allows

investment advisors to keep electronic records in the place of equivalent records in writing if certain disclosures are made. ESIGN's state-level counterparts are governed by the Uniform Electronic Transactions Act ("UETA"), which states that (1) contracts are no less enforceable simply because signatures were provided electronically, or electronic records were used in their formation, and (2) any law that requires that something be in writing may be satisfied by its electronic form. Since ESIGN provides a greater number of concrete provisions than UETA, we will primarily refer to ESIGN when providing insight on how to meet electronic records requirements.

The key to evaluating ESIGN is understanding that it gives electronic records an affirmatory status, such that providing an electronic signature (or otherwise electronically confirming the receipt of records) demonstrates one's understanding of and access to the electronic medium through which the signature was provided. We will use the electronic signature as a robust example of ESIGN regulations at play.

To begin, it is useful to acknowledge that an electronic signature by itself is simply a marking. Therefore, sounds, symbols, and processes such as entering a password or clicking through are all technically electronic signatures. Of course, most contracts require a written signature, and the same would be required of their electronic counterparts. Signatures, electronic or not, should be replicable by their signator. In fact, ESIGN prohibits the use of oral confirmations as signatures. The takeaway here, however, is that electronic signatures alone are not enough to enter into an agreement.[11] For eSignatures to be valid, ESIGN stipulates that they must coincide with a set of disclosures such that the signature itself is an affirmation, and, moreover, an indication, of the user's understanding of these disclosures. All disclosures may be delivered electronically.

ESIGN sets the framework for electronic records to replace paper ones. Its stipulations lean toward an acceptance of the electronic medium for delivering signatures or records. The first set of disclosures required by ESIGN purport that the user has consented to use electronic signatures, understands how to withdraw this consent, and is aware of the consequences of withdrawal. Furthermore, if consent is withdrawn, the eSignature receiver must obtain only information on how to contact the user by another electronic means, such as the user's email.

Secondly, users' provision of an eSignature should indicate their ability to provide affirmations and access records through the same avenue in the future. A conservative approach would be to require users to demonstrate that they could access relevant electronic information in an actual test. At the very least, users should be provided with a statement of hardware and software requirements for accessing and retaining records of signatures and any other records they consented to receive electronically. Users should also be contacted if hardware or software requirements change.

ESIGN also stipulates that the breadth of records to which electronic consent will apply must be disclosed, whether it be only the record at hand or a set of records categories. To sum up, each electronic signature (or electronic form of consent) is setting a precedent for electronic records delivery in the expanding technological landscape.

Implementation

Next, we focus on implementation. Many eSignature providers, by default, retain signed documents in perpetuity on their platforms as long as your account or these documents are not deleted. You may also typically set a retention date, routinely purging documents as you choose. However, sometimes the only means of backing up documents and their associated signatures via eSignature software is to download them to your computer. Nevertheless, eSignature software will still reduce the time advisors spend on entering into agreements and making copies of documents for their records.

Another issue that arises with electronic signature use is authentication. ESIGN contains no specific delivery guidelines. Under UETA, an electronic record is considered sent when it leaves an information system under the sender's control or, if the sender and recipient are using the same system, enters a part of the system under the recipient's control. Correspondingly, an electronic record is received when it enters an information system in the recipient's control. The recipient need not actually access the electronic record for it to be considered received. While eSignature providers may save a complete history of each party's actions with respect to electronic agreements (send, view, print, sign, or decline), protecting parties from back outs after the fact, their user authentication process is not impenetrable.

Exceptions

Other laws specifying records to be delivered in a specific format take precedence over ESIGN and UETA. Electronic records may not be used if they cannot meet the specifications of these other laws. When records must be delivered in a certain format, ESIGN requires clear disclosures to consumers about their right to receive this information in that format. Although the Advisers Act covers most contracts between SEC-registered firms on this point, it is important that state-registered firms familiarize themselves with state laws. Additionally, it is also prudent to ensure that all parties legally entitled to view the record may access it over the duration it must be kept.

[11] Under UETA, any "act by a person" (e.g., a sound, marking, etc.) may be considered that person's signature.

Security breaches and controls

As is always the case with new innovation in technology, attempts to hack and gain unauthorized access to the underlying data happen almost immediately. Fortunately, many of the major eSignature platforms use the most revolutionary advances in security protocol to protect their users and their data. It is best to look for eSignature providers that meet the highest level of security and encryption standards by being International Organization for Standardization (ISO) 27001 and Statement on Standards for Attestation Engagements (SSAE) 16 certified.

ISO 27001 is a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management process. SSAE 16 is a regulation created by the American Institute of CPAs for updating how service companies report on compliance controls.

Despite adhering to the highest levels of encryption and reporting standards, firms remain susceptible to cyberattacks. There have been instances of hackers using targeted spam campaigns to gain access to eSignature providers' systems that contain user data.

Firms using electronic signature services must remain diligent to avoid inadvertently compromising their sensitive data. Precautions that can be taken include the following:

- Keep antivirus software installed on all workstations, and periodically check for security patch updates.
- Use password encryption software to secure all login credentials.
- Do not view or work with sensitive information on public computers or servers. If a public computer must be used, make sure to sign out of all websites and clear the browser cache when finished.
- Avoid phishing emails by being mindful of emails containing files with .zip and .exe file attachments.
- If responsible for firmwide compliance, use training programs, the firm's employee handbook, and regular reviews to reinforce best practices among employees.

Backing up e-data

Outside of cybersecurity, backing up online data is the greatest safeguard against hacking. We have already mentioned that for websites, an update-oriented approach is more user friendly than a time-lapse approach. In addition, because webpages are subject to hacking, it is wise to keep two off-site copies of every webpage instead of the required single duplicate: One may be stored on a computer, and the other in the cloud. If a firm's website is not created on a platform that has a built-in archiving tool, plug-ins that perform this function are available for a variety of website-creation platforms. A firm may look to the recommendations of its service provider to find an archiving system that serves its needs.

Troubleshooting

If data has, unfortunately, been lost, the practices that firms have adopted in anticipation of repercussions may mitigate the severity of the consequences. Keeping a log of where data was first obtained might help a firm crowdsource lost data. For large firms, having a cybersecurity company on hand that can work to recover lost data and conduct penetration tests is advantageous. Schwab has a list of third-party cybersecurity vendors available to serve as a starting point. You may access this list via Schwab's Cybersecurity Resource Center on schwabadvisorcenter.com.

For webpages, the Wayback Machine has been digitally archiving publicly accessible pages on the World Wide Web since 2001.[12] This website crawler copies and saves all information from a public website and all linked public pages, making it a helpful tool for restoring public non-password-protected sites that do not block crawlers. Advisors can block website crawlers by adding the extension "/robots.txt" to their URL and entering customized conditions. Blocking the Wayback Machine will prevent this archiver from crawling new pages and will retroactively render copies of old pages inaccessible.

Corporate records

Corporate structure–related records have unique requirements. Articles pertaining to corporate structure must be maintained in a firm's principal office. Upon termination of a business, all items related to corporate structure, such as partnership articles (and any amendments), charters, minute books, and stock certificate books of the advisory firm and any of its predecessors, must be kept for at least three years.

Regarding business splits and the movement of information to new firms, it is paramount that information that will be used or referenced in the future not leave with departing members. This is most likely to occur when there is client overlap between parties, in which case both parties are required to maintain records on these clients. In fact, protocol information taken by a departing advisor to a new firm counts as a part of these required records, even if clients are not onboarded to the new firm.

[12] This refers to all webpages accessible by web browsers and that otherwise fit the colloquial definition of a "webpage" (on which one can skip from one page to another via links, HTTP is used, etc.). This does not include email, instant messaging, messages sent between servers, etc.

When storing books and records, it is always best to keep organized and err on the side of caution with regards to duration requirements. Most importantly, records should be kept and plans put in place to ensure the successful progress of business.

VI. Conclusion

While we believe that books and records should be kept as proof of fiduciary duty performed by advisors, the goal of the Advisers Act is to ensure that firms act as fiduciaries. Therefore, firms ultimately use records as resources to meet fiduciary standards. An organized set of client records and previous research will save ample time when doing due diligence for future products and services. In fact, if a firm seeks to reduce the books and records it must maintain, the best solution is to prevent problems that require documentation by conducting proper due diligence from the get-go.

Instead of viewing recordkeeping as a duty necessary for preventing negative consequences during an audit, successful firms acknowledge that an organized and integrated recordkeeping system saves them time and resources. For new integration projects, such as mergers or technology adoption, familiarity with books and records endows advisors with key information about their businesses to ensure that transitions go smoothly. Advisors can experience the power of proper recordkeeping by referencing records to make effective decisions, maintaining organized books and records, and ultimately asking themselves whether a document will be useful if kept. These tasks, taken together, will protect not only an advisory firm but also its clients, resulting in the optimal client experience and the accomplishment of fiduciary duty.

As advisors begin focusing on building a firm suitable for scale, prioritizing tax, audit, and regulatory compliance to meet the covenants of being a fiduciary becomes increasingly important. 2017 saw a record 153 mergers and acquisitions deals, while 2018 is on pace to meet or beat that number.[13] With changes to the tax law and an ever-changing regulatory environment, especially regarding the broker protocol, advisors with an eye on strategic growth can use their compliance requirements to best position their operations and their firm.

Online compliance resources

Visit schwabadvisorcenter.com > News & Resources > Compliance for compliance and regulatory information.

Schwab works with third-party firms to provide select resources that help keep you informed of certain regulatory and compliance developments. Access *Compliance Hot Topics*, templates and guideline documents, archived issues of *Compliance Review*, and third-party resources. These resources are complimentary and exclusive to advisors who work with Schwab Advisor Services™.

[13] Devoe & Co., *2017 RIA M&A Activity Slows but Sets a New Record*, (Chicago: Nuveen, 2017).

About the authors

Patrick J. Burns, Jr., JD
President and Co-founder, Advanced Regulatory Compliance, Inc.
Managing Attorney, Law Offices of Patrick J. Burns, Jr., PC

Patrick J. Burns, Jr., is the president and co-founder of Advanced Regulatory Compliance, Inc. He is also the managing attorney with the Law Offices of Patrick J. Burns, Jr., PC, a securities, corporate, and employment law firm dedicated to assisting industry members with their legal needs. Mr. Burns received his juris doctor degree from Southwestern University School of Law in Los Angeles, California, and a bachelor of business administration degree from Pace University's Lubin School of Business in Pleasantville, New York. He began his professional career with a New Jersey–based law firm and then worked in a legal and compliance capacity for several financial services firms located in New York City and Los Angeles. During his financial services career, he acquired numerous Financial Industry Regulatory Authority and insurance licenses. Mr. Burns is a frequent industry speaker on breakaway broker matters, investment advisory compliance issues, and general regulatory matters.

Diana Chen
Compliance Consultant, Advanced Regulatory Compliance, Inc.
Senior Transition Coordinator, Law Offices of Patrick J. Burns, Jr., PC

Diana Chen is a compliance consultant at Advanced Regulatory Compliance, Inc., and senior transition coordinator for breakaway financial advisors at the Law Offices of Patrick J. Burns, Jr., PC. Ms. Chen received a bachelor of arts in psychology and a minor in statistics from the University of California, Los Angeles. She began her career in the finance industry, obtaining her Series 7 and Series 66 licenses. She has since applied her quantitative skills in compliance roles for warehousing, tax, and financial businesses.

Damian Lo Basso
Founder and CEO, Compass CFO Solutions, LLC

Damian Lo Basso is the founder and CEO of Compass CFO Solutions, LLC, a full-service outsourced-CFO and accounting and bookkeeping firm that exclusively serves independent financial advisors. Prior to founding Compass, Mr. Lo Basso served as vice president for alternative asset manager CoVenture and for RIA platform service provider Dynasty Financial Partners. He began his professional career as an investment banker at Deutsche Bank Securities, where he worked in the firm's Structured Credit division. Mr. Lo Basso received a bachelor's degree in accountancy from Providence College in Providence, Rhode Island. He regularly speaks on various topics regarding industry best practices and is a contributor to *Forbes* as a member of the Forbes Finance Council.

The services and/or opinions of the authors listed in this publication are not and should not be construed as a recommendation, endorsement, or sponsorship by Charles Schwab & Co., Inc. or any of its officers, directors, or employees. The authors and firms are independent and not affiliated with or employees of Schwab. You must decide on the appropriateness of the content for you or your firm. Schwab does not supervise these authors and/or firms and takes no responsibility to monitor the advice or consultation they provide to you. This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer or compliance advisor. Any views expressed herein are those of the authors.

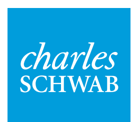
Schwab Advisor Services™ serves independent investment advisors and includes the custody, trading, and support services of Schwab. Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

This material is for institutional investor use only. This material may not be forwarded or made available, in part or in whole, to any party that is not an institutional investor. This article cannot be used, posted, reprinted, or distributed without express written consent from Charles Schwab & Co., Inc.

The services and opinions of the authors are independent of and not endorsed by Charles Schwab & Co., Inc. Neither the firm nor the authors are affiliated with or employed by Charles Schwab & Co., Inc.

©2018 Charles Schwab & Co., Inc. (“Schwab”). All rights reserved. Member SIPC.

JUT (1218-8XN6) NWS15120DEC18-00-00223750 (11/18)



Own your tomorrow.