It’s 2018: Do You Know Where Your Client Data Is?

No financial technology innovation has saved advisors more time than when custodians began transmitting data files to firms.

Prior to this change, client data was updated by taking statements and keying them into the portfolio accounting system. At the end of each quarter, statements were stacked thick and the data entry sprint began so that client reporting and billing could be completed.

Today, these data files circulate through systems that are in many cases developed and hosted by third party fintech companies. Fintechs have been able to take this data and provide additional value and ease of use for firms that seemed hardly imaginable just a couple of decades ago. But that convenience has given rise to new concerns about data security and control.

Last fall I had the opportunity to moderate the Tiburon CEO Consumer Panel. The No. 1 concern brought up by the consumers on the panel was data security. Beyond the concerns of a hacker getting access to passwords, they worried about outright theft due to a security breach. As a result, the consumers complicated their lives by doing business with multiple security firms to help mitigate the risk.

Despite this concern, one detail that clients and advisors alike may overlook is the contractual relationship that exists between custodians, fintechs, advisors, and the client regarding data.

When the advisor asks the custodian to share their data with a third party vendor, is the advisor holding the custodian harmless against breaches that may arise? And, what happens when an advisor authorizes a third party to share the data with, well, another third party? Each of these relationships can be viewed very differently, and as a result the ultimate responsibility for data security may be defined in the small print and not well known.

Knowing where your data ends up is a big deal, not just to your clients but also to your firm, since you may be the one left being asked to make the client whole.

What can be done about it? Let's start by looking at what data is being shared. In most cases, that means files that include a client's name, address, account number, social security number or tax ID, their date of birth and the account value. Essentially, any and all personally identifiable information utilized to safeguard accounts. The keys to the kingdom, so to speak.

Without the sharing of this information, we would go back to the dark ages of manually keying in data. One could argue that in most cases, third party software providers may not need many of these data elements, but in many cases they do. What can be done about it, and what things can we look for to help ensure that client data is protected?

Certainly asking your vendors some questions about security information will help begin to put you at ease:

- Do you encrypt the data at rest in your database?
- Do you have encrypt the data during transit?
- How do you safeguard my data from employee theft?
- Do you offer multifactor authentication for logins?
- Do you have a code scan done to look for vulnerabilities?
- Are you sharing my client data with any third parties (developers, consultants, etc.)
- What do you do to safeguard my client data on your development and test platforms?
- Do you have an SSAE 16 / SOC Type 1 and 2 report that I can review, and how often is this done?
- Do you have an ISO 27001 Certification?
- What other third parties do you bring in to audit the security measures you are taking with my client data?
- Will any of my data be exposed outside of the United States?

If you are thinking that some of the above may not be critically important, imagine telling your client after their funds were stolen that your firm exposed their personally identifiable information to someone outside the country where little if any recourse is available.

If tracking down white collar crime here in our own country is difficult, it's worse elsewhere.

Yes, firms can easily add an extra 20% to their bottom line by offshoring data-related tasks, but how will your client feel about someone in another country having access to their account number, social security, date of birth, and other identifiers without the appropriate security protocols in place?

The current evolution of advisor technology is exciting, but I have significant concerns about where client data is ending up, as well as the general lack of awareness about responsibilities.

If nothing else, please spend some time to understand your contractual agreements as they relate to client data, what the third party vendors that you work with are doing to safeguard it, where your data resides and who specifically has access to it.

This article was originally published on FinancialPlanning.com.

0184-OAS-4/3/2018