RegEd

January 3, 2022

Submitted via email: rule-comments@sec.gov
Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: Request for Comments - File Number S7-19-21 - **Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants**

Dear Ms. Countryman:

On November 18, 2021, the U.S. Securities and Exchange Commission (SEC) published its request for public comment on amendments to the electronic recordkeeping requirements for broker-dealers, security-based swap dealers ("SBSDs"), and major security-based swap participants ("MSBSPs"). The purpose of the rule proposal is to provide an audit-trail alternative to the current requirement that records be preserved exclusively in a non-rewriteable, non-erasable format (write-once, read-many – or "WORM"), and make changes to the designated third-party and notification requirements, along with other modifications. The audit-trail alternative in the rule proposal is designed to address concerns that the WORM requirement causes some firms to deploy an electronic recordkeeping system solely to hold records in a manner that meets the Commission's regulatory requirements for electronic recordkeeping systems.

RegEd, Inc. appreciates the opportunity to comment on this important proposal. RegEd is a RegTech firm whose technology supports broker-dealers, registered investment advisers, banks, and insurance companies with compliance, supervisory and licensing solutions. RegEd's purpose is to enable our clients to create a culture of compliance that serves to protect the retirement savings and investments of individuals. Our firm has more than 200 enterprise clients, including 80% of the top 25 financial services firms, over 1000 clients overall, and our products are used by over 2 million registered representatives, investment adviser representatives, and insurance agents across the United States and beyond.

Some of RegEd's products are designed to facilitate compliance with the electronic recordkeeping standards of 17a-4. RegEd offers feedback and suggestions below on selected items for which the Commission is requesting feedback.

5. Would the proposed rule text setting forth the audit-trail requirement achieve the Commission's objective of imposing an obligation that the electronic recordkeeping system be configured to permit the re-creation of an original record if it is altered, overwritten, or erased? If so, explain why. If not, explain why not and suggest alternative rule text that would achieve this objective.

RegEd believes that the proposed rule text would achieve the Commission's objective to permit the re-creation of an original record, as vendors such as RegEd typically already maintain the audit trail logs with the data points described in the rule. These data points would enable a registrant or our firm to recreate the record at any point in time.

With that said, we would ask for more clarity as to when the Commission believes the audit trail must begin. For example, if a branch is completing a checks received blotter, would the audit trail need to begin when the user *begins* the first entry on the blotter, or would the audit trail begin once the user has submitted and/or saved the first complete entry on the blotter? If a blotter entry was initiated but not all required fields were completed, and the blotter entry draft is subsequently deleted, would an audit trail be required given that this entry never became an official record of the firm?

14. Is the proposed rule text requiring a broker-dealer or SBS Entity using an electronic recordkeeping system to have in place an auditable system of controls that records, among other things: the names of persons inputting, altering, or deleting a record; and the date and time such persons input, altered, or deleted the record appropriate? For example, is this the type of information that could be used to examine whether the system is operating in conformance with the requirements of the proposed rule (e.g., if the electronic recordkeeping system is adhering to the audit-trail requirement, that it is preserving records in a manner that allows the original record to be re-created if overwritten, erased, or otherwise altered)? If so, explain why. If not, explain why not and suggest alternative rule text. For example, is there other information that would be necessary to achieve the objective of the requirement? If so, please identify it. Should the Commission add a requirement for a periodic audit to confirm that the auditable system of controls is working as appropriate? If so, should the required audit be internal or external?

As stated above, RegEd believes these data points to be correct. That said, while the proposed rule contains the data points that must be maintained for the audit trail and broadly states that "Any other *information* needed to maintain an audit trail…" (emphasis ours) must be maintained, the protections that the Commission intends firms to have in place to maintain the *audit trail* data itself are not clear. RegEd would request the Commission provide further guidance on this particular aspect of compliance. The Commission may consider adding language to the proposed rule that states that reasonable controls must be in place to assure that the audit trail data itself is not altered or deleted. Whether or not such a "reasonable" standard is used, we would request that the Commission provide best practices for compliance with the rule proposal with regard to the safeguarding of the audit trail data in addition to the requirement for a backup of such data. We would also request that the Commission confirm whether the Rule 17a-4(f) interpretation in Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, 25282 (May 12, 2003) ("*Electronic Storage of Broker-Dealer Records*") will extend to the requirements for the audit trail alternative.

In its response letter dated December 21, 2021, SIFMA states that "However, by imposing many of the same technical requirements needed to maintain the proposed audit trail alternative to any means of electronic recordkeeping, we are concerned that the Proposed Rules will require WORM solutions to also have the technical requirements of the proposed audit trail alternative, which they many not currently have the ability to do." In agreement with this point, we would suggest the Commission keep the current audit system requirements in 17a-4(f)(3)(v) specific to the WORM alternative in the new rule proposal.

RegEd believes that a requirement for periodic audits should be included, as the rule proposal states that audit results must be provided to regulators but does not provide guidance on the frequency of such audits. Additionally, by requiring audits the Commission will further its goal of affirming that the integrity of data is

protected on an ongoing basis. We also believe that because firms are held to other regulatory standards wherein they must conduct internal audits, that the same methodology of an internal audit could be applied here rather than requiring an external party conduct the audit. However, the Commission should be aware that it will be challenging for registrants to do audits of audit trail data that resides with third-party vendors. This is in part because of the inherent need for those vendors to put access controls in place over the data they maintain. Additionally, if each firm is required to conduct its own audit of the data for each vendor, this would prove costly to the industry and difficult and time-consuming for a vendor to work with each client individually on each periodic audit. Therefore, RegEd believes that if an audit requirement is included, that the Commission should allow firms to rely upon audits carried out by the vendors, either independently or by the vendors themselves. It would be more efficient and less expensive from an industry standpoint for vendors to conduct the audits of their systems on behalf of a large number of firms, as the audit controls and systems will likely be the same for all customers. It lessens the cost and time burden on the industry if it can rely upon audit done by the vendors, while achieving the same objective.

15. Is the proposal to eliminate the requirement that a broker-dealer engage a third party with access to the firm's electronic records who undertakes to provide them to the Commission and other securities regulators appropriate? If so, explain why. If not, explain why not. Further, is the proposal to modify this requirement so that a senior officer of the broker-dealer must have access to the records and undertake to provide them to the Commission appropriate? If so, explain why. If not, explain why not. Should the Commission require that a second senior officer at all times have independent access to and the ability to provide the records and to execute the undertakings? If so, explain why. If not, explain why not. For example, would this increase insider cybersecurity risk compared to the proposed approach? Would switching from a third party to a senior officer reduce cybersecurity risk compared with the current third-party requirement? If so, explain why. If not, explain why not. Would switching to a senior officer provide the Commission and other securities regulators with adequate means to obtain records if the broker-dealer refuses to produce them in the normal course? If so, please explain. If not, explain why not.

RegEd generally agrees that the proposal to eliminate the requirement for a third-party with access to the firm's electronic records to agree to an undertaking, and replace it with the requirement for a senior officer to fulfill that responsibility, is appropriate. However, the senior officer access and undertaking requirement could create new challenges as explained below, and we believe the Commission should consider providing firms with the option to either have a senior officer sign an undertaking or provide an undertaking by a third party, <u>if</u> that third party will also be maintaining those records on behalf of the firm.

While we recognize that part of the intent of this change is to address the issue that the third-party undertaking requirement "needlessly exposes firms to data leakage and cybersecurity threats", we believe the context around those threats was for situations where the firm must engage with an outside third-party solely for the undertaking (a third-party downloader service) where such third-party would not otherwise have access to the firm's records. As an example to the contrary, RegEd serves as the designated third-party for its customers, and our access to those records will not change under the rule proposal because that data resides on servers under our control and oversight.

We believe that there will be challenges for firms and senior officers with the access obligation of the new requirement. For example, because the senior officer is signing a blanket undertaking, he or she will need to obtain access to every recordkeeping system used by the firm. While an individual vendor such as RegEd can create a role to provide the necessary access to an individual, for a senior officer this could ultimately result in

dozens and dozens of logins, many or most of which are to systems that the senior officer does not use on a daily basis. Because the officer does not regularly use the systems, he or she would have to learn the features and functionality for obtaining records and audit trail data from each of these systems and keep up to date on any system changes going forward so that they will be able to comply with the undertaking. It seems like this will create quite a burden on an individual senior officer, particularly given that the undertaking would be invoked in situations where his or her firm is not able or willing to provide the records, which potentially would mean the officer's attention would be pulled elsewhere on urgent firm business or legal issues.

In conjunction with these logins, the senior officer would also be responsible for updating his or her passwords to each of these systems in accordance with each recordkeeping system's password policies, which will be an ongoing administrative burden. Additionally, the senior officer must make sure he or she has appropriate access to all new systems implemented by the firm, which may be challenging in larger firms that implement new systems on a frequent basis. All of these issues would be compounded should the Commission adopt a standard requiring a second senior officer also meet these requirements and have access to all of the same systems. That said, the Commission may consider changing the terminology in the rule from "senior officer" to "designated officers" (as described in the SIFMA response dated December 22, 2021) to allow multiple people, taken together, to cover all means of electronic recordkeeping used by a registrant.

The aforementioned administrative burdens and challenges for the senior officer requirement are heightened by the wording of the rule which states that a senior officer should have such access "at all times".

The senior officer requirement could present challenges to registrants as well. If a senior officer leaves the firm, the firm will need to work with each outside vendor to create access for the new senior officer who will sign the undertaking. Additionally, we would anticipate that firms may wish to have separate legal agreements with vendors for the firm and the senior officer, and so there is the potential for additional administrative burdens caused by having to repaper the senior officer legal agreements with each vendor. Retaining a third-party option would be less of an administrative burden given that these agreements are already in place between firms and third-party vendors.

Another issue with the requirement is that it is unclear as to what level of access the senior officer would require. Specifically, would the senior officer only need access to a front-end interface to retrieve the record and audit trail data, or would he or she need access to the specific databases on which their data is stored? It will be easier for a vendor to provide records pursuant to an undertaking than it is for a senior officer, particularly because end-users typically only have access to the front-end system and not the back-end databases. From a vendor perspective, in order to help protect the integrity of the records and audit trail data, the access controls that are in place are vital to data security, and vendors would need to consider the cybersecurity risk involved in providing an individual with access to the actual vendor database, if that is the Commission's intent.

Most of the aforementioned challenges are more administrative in nature and are in no way insurmountable. However, based on these challenges, we again state our belief that the Commission should consider providing the option for firms to have a designated third-party sign the undertaking in lieu of the senior officer, but only in instances where that third-party is maintaining the records on behalf of the firm. Another option which we believe the Commission should consider is making it acceptable "access" for a senior officer to have a contractual obligation with a third-party recordkeeping vendor to provide on-demand the data which they are maintaining for the firm. In this scenario, the senior officer would not have direct access through the systems, but would have access through a contractual agreement with the vendor, who would provide the data to the

officer. This option could align with the comment made by SIFMA in its December 22, 2021 response: "Thus, SIFMA proposes that 'independent access' in 17a-4(f)(3)(vii) and 18a-6(e)(3)(vii) be change to 'been designated as responsible for providing'."

Finally, should the Commission eliminate the third-party undertaking requirement and replace it with the senior officer standard, we would request that the Commission provide guidance as to whether the existing 17a-4 undertakings signed by third-parties would automatically terminate upon the effective date of the senior officer undertaking requirement of the new rule, or whether there would be a notification requirement or other obligation for a firm to unwind these (e.g., such as removing them from the registrant's financial notifications within WebCRD).

We thank you for the opportunity to provide our feedback and commentary. Should you have any questions, please contact the undersigned via email at [redacted].

Respectfully submitted,

Adam Schaub
Vice President – Product Management, Platform