NCC Group's Response to the Securities and Exchange Commission Request for Comment "Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants" (File Number S7-19-21)

I. Introduction.

NCC Group is a global cybersecurity and software escrow business headquartered in the UK, with a significant market presence in North America, the UK and continental Europe, and a rapidly growing footprint in Asia. Through its recent $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), NCC Group has an established and significant footprint in North America for the software resilience business. The IPM business has been operating in the North American regulatory market for over 30 years including providing designated third party services pursuant to Rule 17a-4 under the No-Action letter since 1993. Accordingly, the designated third party team which joined NCC Group as part of the acquisition of IPM is well versed in the challenges of meeting the requirements of the designated third party rule and the value such services bring in helping ensure compliance with SEC regulations and protecting the interests of investors. Accordingly, now matched with NCC Group's cybersecurity expertise, NCC Group's designated third party team is uniquely positioned to offer the below comments to the proposed rule changes under Rule 17a-4.

II. Proposed Changes to Storage Requirements.

NCC Group is broadly supportive of the proposed changes to Rule 17a-4 which update the references from "electronic storage media" to the more generally applicable term "electronic recordkeeping system." In addition, the proposal requiring the covered entities to maintain a backup set of records is well taken and should be an existing practice among broker-dealers for disaster recovery and business continuity purposes. Lastly, the Commission's addition of an audit-trail based electronic record keeping system appears to be a sensible and workable option in addition to the option to store records in a WORM compliant manner. It appears likely that broker-dealers will benefit from greater access to systems and technology that meet these broader technical criteria.

III. Proposed Changes to the Designated Third Party Requirements for Broker-dealers.

The Commission's proposed rule eliminates the requirement under paragraph (f)(3)(vii) of Rule 17a-4 for a third party to provide regulators with copies of broker dealer records maintained under Rules 17a-3 and 17a-4. Such third party is commonly referred to as a "designated third party." In lieu of the designated third party, the proposed rule would rely on a senior officer in the broker-dealer to provide such records pursuant to an undertaking. Importantly, in the commentary to the proposed rule the Commission notes its belief that such access and undertakings serve a useful purpose, particularly in cases where customer assets are at risk. Accordingly, the question then is which of the two options is the better alternative?

As will be shown, the designated third party is a critical component of Rule 17a-4 which helps to ensure timely access to records if requested by a regulator. The rationale for the proposed elimination of the designated third party requirement is cybersecurity risk and the costs of such services. However,

the risks and costs are overstated and do not favor elimination of the designated third party requirement. In addition, the proposed alternative of reliance upon a senior officer to provide the undertaking is problematic on several levels which decisively undermine its effectiveness. Before addressing these points in detail, it is helpful to review how the designated third party service is performed according to industry best practices.

1. Designated third party service overview.

NCC Group's designated third party service consists of several steps and measures which embody best practices for a designated third party. These steps include the following. Upon execution of an agreement for designated third party services, NCC Group issues a letter of intent. The purpose of the letter is to document that NCC Group, and the broker-dealer are working towards fulfilling the designated third party requirement under the rule. Following the issuance of the letter of intent, the broker-dealer prepares a system configuration plan which outlines the steps required to access the applicable system and records in support of the designated third party requirements. NCC Group then validates the system configuration plan through testing which consists of verifying whether the plan includes all the steps required to access the records in the applicable system. The system configuration plan is tested by following the steps contained within it to access a small sample of records (five records or less, which can include records created for testing purposes) identified by the broker-dealer. Issues identified during testing such as missed steps or missing details are typically resolved during testing by adding the required details to the system configuration plan and continuing testing.

Broadly speaking there are two ways of online testing.[1] First, the broker-dealer can demonstrate the accuracy of the steps outlined in the system configuration plan during a screen share session with the designated third party such as through a WebEx with arrangements for the broker-dealer to provide credentials to the designated third party if needed in response to a request from a regulator. Alternatively, testing may be provided by accessing the broker-dealer's system directly via VPN at the option of the broker-dealer. In such cases, the designated third party may be provided with temporary credentials for use in testing with arrangements for the broker-dealer to provide active credentials if needed in response to a request from a regulator. In some cases, the broker-dealer may provide permanent credentials to NCC Group although it is not specifically required under the rule. In all cases testing occurs only during times scheduled with the broker-dealer and in all cases the broker-dealer is present for the testing including identifying records for testing purposes. In no case, regardless of the chosen means for testing, is an ongoing connection with the broker-dealer application maintained.

Upon completion of the testing, NCC Group issues a test report and a letter of undertaking (as provided in Rule 17a-4) to the broker-dealer for the system. NCC Group follows up twice per year for any updates required to the system configuration plan due to changes in the broker-dealer's IT infrastructure. Testing occurs thereafter on an annual basis.

Any hardware such as laptops, fobs or other devices provided by a broker-dealer to access its application is securely stored in a vault with an auditable chain of custody. Access to the vault is limited

[1] NCC Group has also offered onsite testing at the broker-dealer's location. However, due to the pandemic all testing has been online since approximately Q1/2020. The transition to full online testing occurred with minimal disruption.

to vault personnel through a badge and pin system. The vault is under video surveillance and monitored by an alarm system. In addition, storage is subject to environmental controls (i.e., temperature and humidity) to help assure longevity of stored material and is protected from fire through fire rated construction methods and use of a dry agent fire suppression system (FM-200). These standards employed for vaulting are the same ones used to store intellectual property for banks and large financial institutions.

2. Neither cybersecurity risk nor cost concerns justify elimination of the designated third party requirement.

The proposed rule's commentary cites cybersecurity risk and cost as the key rationales for elimination of the designated third party requirement in favor of an undertaking from a senior officer at the broker-dealer. As shown below, such concerns are overstated and do not justify the proposed elimination of the designated third party requirement.

a. Cybersecurity risk.

The proposed rule's commentary cites cybersecurity threats and risk of data leakage as a key concern in the elimination of the designated third party requirement. As a preliminary note, the current designated third party rule does not require ongoing access to the broker-dealer environment and therefore the risk of data leakage, disclosure of trade secrets, or exposure to cybersecurity threats is inherently minimized. In addition, testing through screen shares (with arrangements to obtain access if required in response to a request from a regulator) requires no access to the broker-dealer's system which virtually eliminates any cybersecurity or data leakage risk.

Even in cases where testing occurs through access to the broker-dealer's system, the cybersecurity risks are minimized in several ways. First, access occurs only on a scheduled basis and with the presence of the broker-dealer during testing. In addition, a small sample (five or less) of records are accessed. Such records are chosen by the broker-dealer and may be records created for testing purposes to validate the system configuration plan. Investor or proprietary information does not need to be accessed to validate that the steps in a system configuration plan are accurate. In many instances, credentials required for testing are activated only for testing and cannot be used to access the system outside of testing.

In certain cases, broker-dealers have opted to provide credentials and hardware required to access their network on an as needed basis. While this level of access is not expressly required under the current rule[2], NCC Group has acquiesced to these requests. In such cases, generally a laptop from

[2] NCC Group does support clarification of the requirements of a designated third party under Rule 17a-4. Although the rule does not expressly require permanent access to the broker-dealer's system by a designated third party, NCC Group's customers have anecdotally reported that they have been required to provide such access to the designated third party and in some cases have reportedly been fined for failure to do so. In other instances, NCC Group's designated third party team has been told by regulators on several occasions that the screen share approach to testing is acceptable and that a means to access the broker-dealer's system on demand is not required as long as arrangements have been made with the broker-dealer to obtain access if required upon request from a regulator. This ambiguity in the rule and the rival interpretations may in fact be driving much of the argument for elimination of the designated third party requirement based on a perceived cybersecurity threat. While NCC Group can support either approach contemplated by these rival interpretations with minimal cybersecurity risk,

the broker-dealer, fob or other type of hardware is required for access. These items are used solely for testing and when not in use are stored in a vault under the conditions outlined above. Given the infrequency of access to the broker-dealer systems coupled with the physical security measures in place for the hardware necessary to access the system, the cybersecurity and data leakage risk is minimal.

In fact, given that hardware provided by a broker-dealer, such as a laptop, would only be used for testing such broker-dealer, the designated third party poses a much smaller cybersecurity risk than a broker-dealer's employee with comparable levels of access. The use of the hardware is minimal and focused only on testing. In contrast, a laptop used by a broker-dealer employee would through normal use be used for answering emails and accessing the internet which are the primary pathways for cybersecurity and data leakage threats. These avenues of exposure to risk do not exist in a typical designated third party engagement which embody the best practices set forth above.

b. Cost.

Cost has been cited as the second basis for eliminating the designated third party requirement. The fees for designated third party services constitute a very small percentage of the overhead of a broker-dealer. In addition, these fees are reasonable and subject to a competitive market for designated third party services with several providers offering services at various price points based on the needs and expectations of the broker-dealer[3]. Fees are driven by the number of systems used by a broker-dealer as well as the number of broker-dealer entities. Thus, broker-dealers with more sophisticated or complex requirements will pay more than smaller broker-dealers with less robust requirements. Accordingly, as with many business expenses, costs are largely driven by the scale of the broker-dealer receiving services. For instance, there are providers available which bundle compliant storage solutions with designated third party services. These providers are an accessible and affordable solution for smaller broker-dealers. Larger broker-dealers require more robust solutions and therefore use dedicated designated third party providers.

3. A Senior Officer Undertaking is not a viable alternative to a designated third party.

The proposed alternative to a designated third party, an undertaking from a senior officer at the broker-dealer, raises substantial questions as to its feasibility. As noted in the commentary for the proposed rule, it is not clear who the officer should be at the broker-dealer. Importantly, such an officer must be in a position to truly be responsible for compliance with the requirements under the proposed rule. However, a senior officer likely may not have the day-to-day technical knowledge to provide the records requested by a regulator. This is especially true in cases of larger organizations with sophisticated IT infrastructure and the potential for needing to access backup records in addition to items in the production environment or in cases where an audit trail for a record is requested by a regulator.

Additionally, the proposed rule contemplates that if the senior officer cannot execute their undertaking, then the broker-dealer will provide an immediate replacement. Importantly, another senior officer may not be available (immediately or at all) and may not have the knowledge or

---

NCC Group would be most supportive of clear guidelines permitting the designated third party to rely on an arrangement with the broker-dealer to provide access if requested by a regulator.

[3] For instance, internal market research conducted a few years ago found at least nine competitors offering designated third party services.

credentials to access the required records which would defeat the purpose of the proposed rule. The senior officer approach contemplated in the proposed rule introduces a single point of failure reliant upon a single individual.

Further, reliance upon the senior officer is problematic if they believe they are the subject of an investigation or inquiry. The officer may frustrate the request for records through a number of means including providing portions of requested records or failing to obtain required information or credentials to access systems. The officer may also attempt to invoke their Fifth Amendment privileges which would further impede a regulator's access to the system. Such a scenario presents an unacceptable delay if customer assets are at risk.

Lastly, the broker-dealers may fail to designate a successor senior officer to replace one that has left the firm in the ordinary course of business. This is particularly likely in a large broker-dealer supporting many broker-dealer entities in a dispersed organization. As a designated third party, NCC Group's experience is that in such organizations it is not often clear who is responsible for a given application and it may take months to determine the responsible internal resource for an application when arranging an annual test. These challenges would be compounded if such organizations became solely responsible for managing the undertaking requirement. Without a dedicated designated third party, these requirements may be easily overlooked particularly when coupled with changes in IT infrastructure. The resulting confusion may only come to light due to a request from a regulator and would result in detrimental delays in cases where time is of the essence.

A designated third party by contrast is an organization rather than an individual and therefore much better positioned to provide access to records without interruption due to routine staff turnover. In addition, the designated third party would not face any conflicts regarding the scope of an investigation or inquiry and truly provide a regulator with an independent means to access records stored under the rule. Perhaps most importantly, the designated third party best practices outlined earlier provide a paper trail, accessible to regulators during an audit, to demonstrate compliance with the spirit and letter of the rule. This trail includes the letter of intent, letter of undertaking, the system configuration plan, annual test reports and any updates to the system configuration plan during the year. These documents provide transparency and demonstrate a high level of readiness to support a regulator if needed. The proposed rule provides no similar mechanism to show compliance with the regulation.

IV. Conclusion.

The proposed rule provides important updates to language and technical requirements for storage, which NCC Group supports. However, the additional proposal to eliminate the designated third party requirement would be a great error. Since its inception, the designated third party requirement under Rule 17a-4 has served an important function in helping ensure that the regulators have timely access to records in support of investigations and inquiries necessary to uphold the integrity of the market and protect the interests of investors. The impact of a designated third party extends beyond merely providing records to a regulator upon request because it creates a clear incentive for full cooperation from broker-dealers at the outset by providing an alternative and independent means to access records if the broker-dealer fails to do so. The Commission notes in its commentary the apparent value of an undertaking for accessing records in a timely manner. The only question then is which

approach is the better alternative? As shown above, the designated third party offers decisive advantages in protecting investors and the integrity of the marketplace. This important tool for regulators should therefore remain in place.