



Computershare
1290 Avenue of the Americas 9th Floor
New York New York 10104
Telephone 1 212 805 7100
www.computershare.com

June 5, 2023

Vanessa Countryman, Secretary
U.S. Securities and Exchange Commission
By email: rule-comments@sec.gov

Re: Securities and Exchange Commission Release No. 34-97142 (the “Release”) **File Number S7-06-23, Cybersecurity Risk Management Rule** for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents (the “Proposed Cybersecurity Rule”)

Dear Secretary Countryman:

Computershare Limited, on behalf of itself and the U.S., Canadian and Hong Kong registered transfer agent affiliates and U.S. registered broker-dealer affiliate described below (“Computershare”), appreciates the opportunity to provide comments to the Securities and Exchange Commission (the “Commission” or “SEC”) on the Proposed Cybersecurity Rule relating to the management of cybersecurity risks.

Computershare Limited (ASX: CPU) is a global market leader in transfer agency and share registration, employee equity plans, mortgage servicing, proxy solicitation and stakeholder communications. We also specialize in corporate trust and a range of other diversified financial and governance services. Computershare is represented in all major financial markets, with Computershare US and Computershare Canada combined servicing over 25,000 transfer agency clients and over 18 million registered securityholder accounts.

Within the Computershare family, Computershare Inc., Computershare Trust Company, N.A., and Computershare Delaware Trust Company (collectively, “Computershare US”) are registered transfer agents located in the United States. Computershare Trust Company of Canada and Computershare Investor Services, Inc. (collectively, “Computershare Canada”) are registered transfer agents located in Canada. Computershare Investor Services Limited (Hong Kong) is a registered transfer agent located in Hong Kong (“Computershare HK”). Georgeson Securities Corporation is a registered broker-dealer.

I. GENERAL COMMENTS

Computershare agrees with and supports the position of the Securities Transfer Association (“STA”) in its comment letter to the Commission dated June 5, 2023 (the “STA Comment Letter”).

We note that Computershare US takes an active role in this industry organization through membership on the Board and various committees and participated in the development of the STA Comment Letter.

Computershare, however, would like to offer its additional comments and recommendations on certain items where it has a particular interest or concern, or a unique view including due to its global enterprise. Computershare believes that for many transfer agents, the Proposed Cybersecurity Rule is unnecessary as such transfer agents are already subject to state, federal or provincial laws addressing information security and cybersecurity risk. Computershare further believes certain provisions of the Proposed Cybersecurity Rule are unduly burdensome, and that compliance with other provisions will be difficult, if not impossible, to achieve.

Computershare notes that on the issue of addressing cybersecurity risk, it provided comments to the Commission's Concept Release and Request for Comment on Transfer Agent Regulations¹ by letter dated April 14, 2016 (the "2016 Comment Letter"). As stated in the 2016 Comment Letter, Computershare believes information security of recordkeeping systems for transfer agents is critical. It supports the Commission in its endeavors to modernize rules applicable to transfer agents to address the cybersecurity risks presented by electronic recordkeeping and to protect against unauthorized access to personal information. However, Computershare had concerns regarding certain aspects of cybersecurity rules and will reiterate these concerns as well as additional concerns with the Proposed Cybersecurity Rule herein.

Given the breadth of the changes required under the Proposed Cybersecurity Rule, Computershare supports the STA's recommendation that any final rule includes a minimum of 24-36 months' compliance period to ensure covered entities have sufficient time for the development and implementation of policies and procedures needed to meet the new requirements.

II. EXISTING CYBERSECURITY LAWS GOVERNING TRANSFER AGENTS

As noted in the 2016 Comment Letter, there is a litany of existing state and federal laws and regulations already governing transfer agents in the performance of their transfer agency and related services, including laws relating to cybersecurity and information security. While the Commission recognizes this in the Release, the Proposed Cybersecurity Rule provides conflicting requirements with other federal and state laws.

A. Banking Laws

Many registered transfer agents like Computershare US and Computershare Canada entities are banks or trust companies, and therefore already subject to state, federal, or provincial banking

¹ Concept Release and Request for Comment on Transfer Agent Regulations Name of Release, 60 Fed. Reg. 81,948 (Dec. 31, 2015).

laws, rules, regulations and inter-agency guidelines. For such agents, banking law already addresses the various components of the Proposed Cybersecurity Rule, including policies and procedures, risk assessments, and incident reporting.²

Computershare would request that bank and financial institution transfer agents already subject to existing banking laws (whether US or non-US, as applicable) addressing cybersecurity risk be exempt from the Proposed Cybersecurity Rule. It would not only be challenging from a compliance standpoint, but also burdensome to have to comply with multiple sets of similar but different rules on the same topic. In addition, having separate sets of rules could become problematic if the transfer agent is examined by multiple regulators with respect to such rules, and the regulators provide different or conflicting interpretations or guidance. Just as the Office of the Comptroller of the Currency (“OCC”) has a rule that defers to the Commission’s rules as they relate to operational and reporting requirements for transfer agent activities of registered national bank transfer agents,³ the Commission could defer to bank regulations for transfer agents subject to such regulations on cybersecurity. This would avoid duplication of regulations, and still ensure all transfer agents have appropriate regulations in place governing such matters.

B. State and Foreign Laws

In addition to banking laws, many states have enacted legislation addressing information security and data privacy. For example, Massachusetts has had regulations in place since 2010 requiring companies handling Massachusetts’ residents’ information to implement an information security program to protect data.⁴ In the past five years, nine (9) states⁵ have enacted data privacy laws which include provisions relating to protection of personal information and information security. All states have breach notification laws in place to notify their residents of unauthorized access to their residents’ data.

Foreign jurisdictions such as the European Union, Canada, and Hong Kong also have data privacy laws addressing information security and breach notification.⁶ Transfer agents are subject to such

² See, e.g., 12 C.F.R. § 30, Appendix B to Part 30 – Interagency Guidelines Establishing Information Security Standards; Computer Security Incident Notification Requirements, 12 C.F.R. § 53 (OCC), 12 C.F.R. § 225.300-225.303 (Federal Reserve System), 12 C.F.R. § 304.21-304.24 (FDIC); OCC Bulletin 2022-8, Information Technology: OCC Points of Contact for Banks’ Computer-Security Incident Notifications (March 29, 2022), <https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-8.html>; New York State Department of Financial Services Cybersecurity Regulation, 23 NYCRR Part 500.

³ See 12 C.F.R. § 9.20.

⁴ 201 Code Mass. Regs. § 17.

⁵ https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

⁶ See, e.g., <https://www.elegislation.gov.hk/hk/cap486> (the ordinance) and https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html (the regulator) for Hong Kong; and The Personal Information Protection and Electronic Documents Act (PIPEDA), a federal privacy law for Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/.

laws either directly (in the case of non-US registered transfer agents) or indirectly as agents or as “service providers” or “processors” for their issuer clients.

As noted in the STA Comment Letter, absent preemption of state law by the SEC when state laws conflict with the Proposed Cybersecurity Rule, or exemption with respect to transfer agents subject to banking laws, it will be extremely challenging for transfer agents or other covered entities (as defined in the Proposed Cybersecurity Rule) to comply with both sets of laws. Likewise, it will be challenging for non-US transfer agents who are covered entities to comply with potentially different and redundant foreign laws.

III. PROPOSED CYBERSECURITY RULE

A. Cybersecurity Policies and Procedures (§ 242.10(b)(1))

While Computershare supports transfer agents having written policies and procedures to address cybersecurity risks, we have recommendations to clarify, reduce the burden and associated costs of, or address the impracticality of certain provisions of Proposed Cybersecurity Rule 10(b)(1).

Information Protection, Measures to Monitor Systems (§ 242.10(b)(1)(iii)(A))

The information protection section of the policies of procedures requires covered entities to have “measures designed to monitor the covered entity’s information systems and protect the information residing on those systems from unauthorized access or use”

It is unclear what level of monitoring is expected under this section of the Proposed Cybersecurity Rule, and the frequency of such monitoring. Computershare recommends that the Commission provide examples or further guidance on what measures to monitor would be deemed sufficient to meet this proposed requirement.

Information Protection, Oversight of Service Providers (§ 242.10(b)(1)(iii)(B))

This section requires covered entities to have policies and procedures requiring “oversight of service providers . . . pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of this section, that are designed to protect the covered entity’s information systems and information residing on those systems.”

Requiring transfer agents to include in their contracts with vendors that such vendors have policies and procedures that essentially meet the Proposed Cybersecurity Rule is impractical and would present a significant challenge for compliance. Even if this requirement is applied prospectively (for which we would seek clarification), we would expect vendors to object to such provisions as

they are not subject to the Proposed Cybersecurity Rule, may not be subject to the jurisdiction of the SEC, and would have their own policies and procedures to protect personal information that may differ from the requirements under the Proposed Cybersecurity Rule.

B. Annual Review of Policies and Procedures (§ 242.10(b)(2))

Proposed Cybersecurity Rule 10(b)(2) requires an annual review of the covered entity's cybersecurity policies and procedures to ensure they are effective and up to date with changes in cybersecurity risks. While such a review is reasonable and appropriate, the Proposed Cybersecurity Rule further requires that a written report be created that "describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report." Such a requirement to create a separate document covering the various review components is superfluous and may require significant time and effort and coordination by multiple departments. Covered entities should have the flexibility to document their compliance with the annual review requirement in whatever means is most effective, including through documentation that was already created as part of their review.

C. Notification and Reporting of Significant Cybersecurity Incidents (§ 242.10(c)) and Definition of Significant Cybersecurity Incident

Computershare does not object to notifying the Commission of significant cybersecurity incidents (subject to our commentary below on the definition of such incidents) but believes the reporting process set forth in Proposed Cybersecurity Rule 10(c) should be revised and streamlined. Computershare believes immediate notification after determination that a significant incident has occurred is unreasonable, as a covered entity's resources should be dedicated to investigation, remediation, and resolution rather than giving immediate notification to a regulator and having to compile data to complete a form. We would recommend that notification be required promptly or as soon as practicable. We further recommend the time to file Part I of Form SCIR is upon completion of the covered entity's review and analysis of the incident, and no later than (30) thirty days, as notification would have already been given, and the form merely memorializes and expands on information previously given to the Commission. Computershare further recommends the Proposed Cybersecurity Rule be revised to exempt notification to an appropriate regulatory agency ("ARA") if the ARA has already been informed pursuant to other regulatory requirements.

Computershare also believes it is burdensome to require covered entities to make subsequent filings of Part I of Form SCIR within 48 hours when any information in the previously filed form becomes "materially inaccurate," when new material is discovered, when the incident is resolved, or an internal investigation is closed. Filing an updated form when the incident is resolved would seem sufficient to notify the Commission the matter is no longer a concern. It is not clear what benefit the Commission will gain from continual updates being filed with the Commission while a covered entity is dealing with a significant incident.

In connection with reporting of significant cybersecurity incidents, Computershare would also note the definition of “significant cybersecurity incident” is overly broad in that, as currently written, it would apply to one individual securityholder who has had unauthorized access to his/her information that is reasonably likely to result in substantial harm. This definition is not aligned with other cybersecurity incident notification laws⁷ which require a much higher standard of harm to trigger notification and may result in significant numbers of reports being made for individual incidents with no material impact on the covered entity. Having to annually report all such individual incidents on Part II of Form SCIR may unnecessarily alarm market participants and distort the actual risk profile of a covered entity. We would recommend changing this standard to align with other industry definitions.

D. Disclosure of Cybersecurity Risks and Incidents (§ 242.10(d))

For the reasons set forth in the STA Comment Letter, Computershare does not support the requirement for transfer agents to publicly disclose its cybersecurity risks and measures to address them on Part II of the proposed Form SCIR. This provides no meaningful information to securityholders who do not choose transfer agents and presents a risk that wrongdoers would use such information to identify and act upon system vulnerabilities, in complete contravention of the intent of the Proposed Cybersecurity Rule to enhance the protection of information systems and information residing thereon. While the Commission notes that the intent of Part II of proposed Form SCIR is to keep the disclosures “high-level” so they do not increase cybersecurity risk,⁸ if this is the case, it raises the question of the value of the report and whether it really provides any meaningful information about a covered entity’s risk profile.

E. Rule 17Ad-7, Record Retention

Computershare has comments on two of the provisions of proposed changes to Rule 17Ad-7. With respect to retention of written policies and procedures required under the Proposed Cybersecurity Rule, changes include that transfer agents maintain these “until three years after the termination of the use of the policies and procedures.” This language is unclear as standard practice would be to amend or update policies and procedures, rather than terminate them. Computershare seeks clarification on whether the intent to retention after termination of the procedures was for transfer agents to maintain original policies and procedures for three years after amendments are made.

⁷ See, e.g., 23 NYCRR Part 500.17 (requires notification of the incidents “that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity”); 12 C.F.R. § 53.2(7)(“Notification incident is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization’s— (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.”).

⁸ Cybersecurity Risk Management Rule, 88 Fed. Reg. 20212 (April 5, 2023), at 20256.

Proposed changes to Rule 17Ad-7 also require “written documentation of the occurrence of a cybersecurity incident” be maintained for three years. Computershare believes that this requirement should only apply to significant cybersecurity incidents (subject to Computershare’s recommended modification of the definition), as it otherwise would include potentially many items that are minor in nature and not the fault of a covered entity. For example, retention of documentation could include a report of an external identity theft occurring that permitted a wrongdoer to get into a securityholder account (through no act or omission of a covered entity, as the wrongdoer had the securityholder’s credentials). We believe it would be burdensome to have to maintain a separate record of such items for three years and do not see the benefit of doing so for securityholders, our issuer clients, or Computershare.

IV. CONCLUSION

Computershare supports the Commission’s goal to enhance cybersecurity in the securities industry for all market participants and supports certain of the Proposed Cybersecurity Rule requirements. For the reasons set forth above, we believe the Commission should consider exempting transfer agents from the Proposed Cybersecurity Rule where existing federal or state bank regulatory requirements already govern such transfer agent entities, as well as consider preemption of duplicative and conflicting state law. As set forth in the STA Comment Letter, if the Commission does not intend to use its preemption authority, we believe it should provide a cost-benefit analysis identifying the specific ways in which the Proposed Cybersecurity Rule would be an improvement over existing regulations. In addition, Computershare would request the Commission consider its other recommendations for changes set forth herein.

Computershare truly appreciates the opportunity to comment on the Proposed Cybersecurity Rule. As noted in the STA Comment Letter, in view of the brief time period permitted to provide comments to the proposed Cybersecurity Rule, we were unable to address all of the questions posed by the Commission but would be glad to answer any questions directly or to further discuss with the Commission the Proposed Cybersecurity Rule and Computershare’s comments herein.

Sincerely,

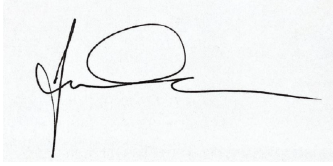


Ann M. Bowering
CEO US Issuer Services, Computershare Inc.



Frank A. Madonna
President, Computershare Trust Company, N.A.
and Computershare Delaware Trust Company
CEO, Computershare Corporate Trust Integration

Vanessa Countryman, Secretary
Securities and Exchange Commission
Page 8
June 5, 2023

A handwritten signature in black ink, appearing to read 'Irfan Motiwala', is displayed on a light gray rectangular background.

Irfan Motiwala
CEO Issuer Services, Computershare Trust Company of Canada and
Computershare Investor Services, Inc.

A handwritten signature in black ink, appearing to read 'Richard Houg', is displayed on a light gray rectangular background.

Richard Houg
CEO Issuer Services, Asia
Computershare Investor Services Limited (Hong Kong)

cc (by e-mail): Moshe Rothman, Assistant Director
Mark Saltzburg, Senior Special Counsel
Catherine Whiting, Special Counsel
Elizabeth de Boyrie, Counsel
Division of Trading and Markets