Abhay Raman
SVP & Chief Information Security Officer

Sun Life Financial Inc.
1 York St.
Toronto ON M5J 0B6

Honorable Gary Gensler, Chair
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Chair Gensler,

We appreciate the opportunity to comment on the U.S. Securities and Exchange Commission's (SEC) proposed rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies. We support the submission of the American Council of Life Insurers to this consultation, and respectfully submit this additional letter for your consideration.

Sun Life is a leading financial services organization providing insurance, wealth, and asset management solutions to individual and corporate clients in several countries around the world. Through SLC Management, our affiliated asset management business, we are a large asset manager with experience in fixed income, real estate, infrastructure, and alternative credit.

We welcome the SEC's attention toward ensuring that investors have access to decision-useful information on how companies are effectively managing risks from cybersecurity attacks. This is a concern deeply held by Sun Life as an investor.

As an issuer, data security is key to our value proposition. Our clients trust us with their sensitive health and financial data. We cannot deliver value to our clients if we do not have their trust.

We are continually evolving our cyber defenses to be effective against emerging cybersecurity threats. We are also delivering comprehensive training on data protection to our employees, contractors, and advisors, implementing new security safeguards and embedding privacy protection in our culture and processes.

As a Canadian-headquartered company, we are subject to strict regulatory obligations concerning cyber risk management and incident reporting by securities regulators. The Canadian Securities Administrators have issued comprehensive guidance that lays out clear expectations for issuers to provide risk disclosure if they are exposed to material cyber risks and develop cyber-attack remediation plans that include disclosure guidelines for material cyber-attacks.

In addition, many Canadian multinationals are supervised by regulators that issue cybersecurity frameworks and requirements that are tailored to their size and industry. Our federal regulator, the Office of the Superintendent of Financial Institutions has taken several steps to ensure Canadian financial institutions are resilient to cyber-attacks. Some of these measures include:

- piloting "intelligence-led cyber resilience testing" to test the cyber resiliency of institutions.

- publishing an updated cyber security self-assessment tool and enhanced Technology & Cyber Incident Advisory reporting requirements; and
- updating Draft Guideline B-13*, Technology and Cyber Risk Management* that sets out expectations for technology and cyber risk management.

Finally, many Canadian companies can report cybersecurity incidents to Canada's cryptologic agency, the Communications Security Establishment through the Canadian Centre for Cyber Security.

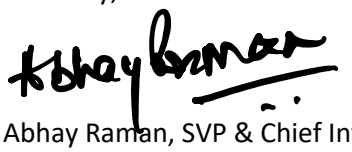
Due to the significant regulatory obligations Canadian companies are already subject to, we urge the SEC to continue to permit eligible Canadian foreign private issuers to follow domestic disclosure standards and documents to satisfy the Commission's requirements and to make any compliance with SEC rules strictly voluntary for MJDS filers.

Not doing so would subject Canadian companies to additional incident reporting regimes that would distract critical resources with fulfilling reporting obligations rather than focusing on addressing a cybersecurity incident. In addition, duplicative disclosure requirements would increase the regulatory burden on companies without necessarily meeting the SEC's aims.

We encourage the SEC to work closely with Canadian regulators to resolve any concerns with existing cybersecurity reporting regimes before imposing additional reporting requirements. Cross-border regulatory cooperation is a powerful tool to support regulators seeking to fulfill their mandate while also minimizing disruption to businesses.

We look forward to working collaboratively with the SEC on cybersecurity risk management, strategy, governance, and incident reporting. Please let me know if you have any questions or if there is any way we can be of further assistance.

Sincerely,



Abhay Raman, SVP & Chief Information Security Officer