Keith Kleiman
Senior Vice President, Chief Information Security Officer
T 212.251.5484

333 West 34th Street
New York, NY 10001-2402
segalco.com

June 12, 2023

David Jensen
911 Ridgebrook Rd.
Sparks, MD 21152

Re: DOL Cybersecurity Response

Dear David:

My name is Keith Kleiman and I am Segal's Chief Information Security Officer. My colleague, Matt Jackson, forwarded to me your request for information on Segal's cybersecurity and data protection program. As demonstrated below, Segal undertakes reasonable commercial efforts intended to prevent the unauthorized use or disclosure of UFCW Giant - Variable Annuity Fund data.

Segal is committed to protecting the confidentiality, integrity and availability of data entrusted to us by our clients. As part of that commitment, Segal has adopted Information Security Policies, which define administrative, physical and technical safeguards, as well as Information Security controls intended to meet various regulatory and legal requirements. Components of Segal's Information Security Program include but are not limited to:

- Data Security Governance Committee
- Board of Directors Information Security Briefings
- Information Security Governance
- Chief Information Security Officer
- Policies and Procedures
- Education and Awareness Communications
- Data Classification and Handling
- Internal / External Vulnerability and Penetration Tests
- Risk Assessments
- Incident Management and Response
- Secure Data Centers
- Security Event Log Monitoring and Alerting
- Data Access Management
- E-mail, Web and AntiSpam Filters
- Secure File Transfer
- Next Generation Firewalls
- Intrusion Prevention Systems (IPS)

- Mobile Device Management
- Malware Protection
- Virus Protection
- Workstation Encryption
- Dual Factor Authentication
- Single Sign On
- Identity and Access Management
- Data Loss Prevention (DLP)
- Removable Storage Controls

In addition, Segal has implemented electronic and procedural mechanisms to identify and respond to suspected or actual security incidents, and mitigate, to the extent practicable, harmful effects of security violations and other security events. Mechanisms include a formal incident response plan. This plan is tested annually and identifies the roles and responsibilities of all Security Event Response Team members, as well as the responsibilities of management, and coordination between participating departments. It outlines the appropriate incident response procedures that should be undertaken in the event of a suspected incident, including but not limited to mandatory data breach reporting requirements.

Additional information on Segal's cybersecurity and data protection efforts is provided in the attached "Segal Information Security Program Summary 2023". If you require additional information, please let us know.

Sincerely yours,

Keith Kleiman

Keith Kleiman
Senior Vice President, Chief Information Security Officer