BUSINESS CONTINUITY DISCLOSURE

Important Information About Business Continuity

Victory Capital Services, Inc. ("VCS") has adopted the business continuity plan of its affiliated registered investment advisor Victory Capital Management Inc. ("Victory Capital"). The following is a summary of Victory Capital's Business Continuity plan.

Victory Capital maintains a Business Continuity Plan ("BCP") that addresses business continuity, disaster recovery, information security and cybersecurity defenses in order to satisfy Victory Capital's obligations as an investment advisory firm registered with the Securities and Exchange Commission (SEC), a registered commodity pool operator (CPO) with the Commodity Futures Trading Commission, and other best practices. Victory Capital's BCP shall be reasonably designed to safeguard its information and that of its clients from loss, alteration, or destruction and to protect the interests of clients from risks resulting from Victory Capital's inability to provide advisory services following a natural disaster, cybersecurity attack or other business continuity or information security threat.

1. Organizational Responsibility

The BCP is owned and maintained by the Technology and Operations Department, under the supervision of the Chief Technology Officer. The contents and implementation of the plan are facilitated by managers of other departments and by external service providers, in coordination with Technology and Operations. Victory Capital's Chief Compliance Officer ("CCO") shall ensure the plan is in place and tested at least annually.

Victory Capital has established an Information Security Governance and management structure to provide strategic alignment with the firm's business objectives, assess information security risks, implement corresponding policies for risk mitigation, and to provide oversight of the effectiveness of the firm's Information Security Program.

The employees of Victory Capital are responsible for protecting client and firm assets in accordance with stated policies and procedures as well as good common sense. This includes proper storage of data and locking computers when not in use as well as utilizing password protection or encryption technologies when transmitting sensitive client or firm data.

2. Risk Assessments

Victory Capital's Technology and Operations Department, in coordination with the firm's Risk Management Committee, is responsible for assessing firm risks at least annually and ensuring adequate controls are in place. Risk assessments are periodically performed on Victory Capital's

facilities and operations to determine levels of threats and risks facing each site and to identify opportunities for mitigation. Victory Capital continuously strives to strengthen our BCP assessment processes through periodic program adjustments, ensuring Victory Capital's most critical functions are properly identified and prioritized.

3. Design and Testing

Victory Capital has adopted multiple Information Security policies designed to articulate the firm's cybersecurity strategy, and ensure appropriate measures are taken to protect and preserve firm data and systems. Victory Capital's BCP is designed to holistically examine Victory Capital's operations and plan against the loss of personnel, facilities and technology that support Victory Capital's business processes. In order to protect our assets, Victory Capital has the following controls in place to mitigate unwanted risks:

- Physical controls where appropriate, such as building security, doors with access controls and locked cabinets in place to guard against common threats;

- Logical controls, such as user access credentials and two-factor authentication in place and maintained in accordance with the firm's security standards; and

- Information security controls, such as identity and authentication systems, firewalls, secure networks, data encryption, data backup and anti-virus software.

Victory Capital tests the BCP annually (or more frequently if material changes occur) to ensure continuity and sustainability. The CCO and Risk Management Committee provide oversight and review of the plan and ensures that the plan is tested at least annually. Test results are used to identify missing or ineffective controls and to improve overall coordination and design of the BCP. Testing methods vary from walk-throughs to full- scale testing exercises in coordination with our business partners.

4. Third Party Oversight

Contracts with third party service providers contain provisions requiring third parties to meet certain business continuity objectives and may contain more or less stringent language depending on the nature of the relationship and the service being provided. Managers responsible for critical vendor relationships conduct due diligence at least annually in order to confirm that the policies and procedures of such third-party service providers are reasonably designed to identify and guard against potential disasters and information security risks.

Victory Capital has partnered with a global outsourcing partner, Cognizant Technology Solutions, to manage and monitor our information security and cybersecurity environment. The Cognizant

Security Operations Center (SOC) provides continuous 24x7x365 monitoring of our information systems and tracks the latest published risks to forecast cyber risk in our environment. When necessary, the SOC team will respond to events with the appropriate corrective actions.

5. Program Adjustments and Training

The Technology and Operations Department reviews Victory Capital's BCP on a periodic basis and adjusts it as necessary to ensure its continued appropriateness and effectiveness. Factors that may influence adjustments include new risk profiles, risk assessments, acquisitions, new regulatory requirements, testing results and feedback from internal or external sources.

Victory Capital's Technology and Operations and Legal, Compliance and Risk Departments periodically educate employees regarding business continuity, information security and potential cybersecurity threats. Mandatory security awareness training is provided to all employees.