

SUMMARY OF INFORMATION SECURITY AND PRIVACY CONTROLS

Provided by **Global Financial Services, L.L.C.**, and **GFS Advisors, L.L.C.**, (collectively “Global”).

How Global Protects Your Privacy

At Global, we recognize the importance of maintaining your personal and confidential information. Ensuring that your information is secure is core to our business. Global maintains privacy policy and procedures designed to protect the personal nature of the information you have entrusted to us. From technology safeguards to employee policies and operating procedures, we maintain constant vigilance where your privacy is concerned.

Account Protection Resources:

- **Raymond James** (primary clearing Broker-dealer) – [Keeping your Account and Personal Information Secure;](#)
- **Morgan Stanley** (offers execution and custody for certain advisory relationships) – [Privacy Pledge;](#)
- **Pershing** (offers execution and custody for certain advisory and broker-dealer relationships) – [Privacy Statement;](#)
- **FINRA** (self-regulatory agency dedicated to protecting investors and safeguarding market integrity) – [Investor Alert: Keeping Your Account Secure: Tips for Protecting Your Financial Information;](#) and
- **U.S. Securities and Exchange Commission** (serves to protect investors while maintaining fair, orderly, and efficient markets) – [Investor Bulletin: Protecting Your Online Investment Accounts from Fraud.](#)

Physical Security

At our office in Houston, Texas, our facility provides physical and electronic measures to secure our building and limit access to our floor. Security officers are onsite 24 hours a day; visitors must be identified and granted access.

Information Technology (“IT”) Security

We maintain strict controls to limit and control access to our network. Our network is monitored around the clock for signs of tampering or unauthorized activity. We employ encryption, virtual private networks, penetration and vulnerability testing, and the latest firewall and antivirus technology. Email monitoring is also utilized for regulatory and compliance purposes.

Incident Response

Global has specialized programs to prevent and detect intrusion, including an incident response program. Our incident response team, which includes both internal and external IT consultants, ensures that appropriate technology and resources are dedicated to preventing and monitoring cyberthreats.

Technology Risk Management

Confidentiality, integrity, and availability of our IT systems and client data are of the utmost importance to Global. Global employs a risk-based control framework to protect our systems and data according to the nature and sensitivity to mitigate the risk from cyberthreats and vulnerabilities. Backup Servers are mirrored offsite every

SUMMARY OF INFORMATION SECURITY AND PRIVACY CONTROLS

30 minutes; this enables us to restore servers or individual files to any 30-minute point in time over the prior 24-months. IT risk assessments are conducted periodically, and any outstanding remediation items are addressed and monitored.

Employee Training

Our employee policies emphasize the importance of cybersecurity and preserving client confidentiality. To reinforce our policy and keep employees current, all employees must complete annual continuing education on a range of topics, including cybersecurity. Our compliance and senior management also ensure that we meet federal and regulatory requirements for maintaining client privacy.

Business Continuity

Compliance and senior management continually focus on preparing for and mitigating potential business disruptions due to unforeseen circumstances such as significant weather events or other natural disasters. Our goal is to ensure that critical operations continue, and data remains secure during any emergency. Global maintains a remote location for continuing operations and emergency functions such as data retention, backup, and offsite information storage. See our [Business Continuity Plan – Disclosure Statement](#) for additional information.