Retirement plan services

Cybersecurity

CAPITAL GROUP® | AMERICAN FUNDS®

Your security is our priority

Trillions of dollars in assets and the sharing of sensitive information online between entities make the retirement plan industry an especially ripe target for cybercrime.

To help plan sponsors, recordkeepers and others mitigate risks, the U.S. Department of Labor (DOL) provides cybersecurity guidelines for ERISA-covered retirement plans, including:

- **Tips for hiring a service provider** with strong cybersecurity practices for plan sponsors and fiduciaries.
- **Cybersecurity program best practices** to manage risks for plan fiduciaries and recordkeepers.
- **Online security tips** to help participants reduce the risk of fraud and loss.

On the next page, learn more about the comprehensive security measures that we've put in place for our RecordkeeperDirect® and PlanPremier® retirement plan solutions.

Investments are not FDIC-insured, nor are they deposits of or guaranteed by a bank or any other entity, so they may lose value.

Capital Group cybersecurity

We have an extensive cybersecurity program that's continually monitored and updated. Here are some highlights of what we already have in place to align with the DOL guidelines:

Dedicated people

Cybersecurity is managed and executed by highly trained professionals with clear roles and responsibilities:

- Our Chief Information Security Officer leads our efforts to manage technology-related risk.
- We have dedicated cybersecurity teams with most members holding industry-standard certifications, such as CISSP training.
- Our employees are trained regularly on how to prevent, detect and respond to cyberthreats and attacks.

Third-party experts

We use independent, industry-leading vendors to help with:

- Fraud prevention and detection, technology and risk assessment, and 24/7 global event monitoring.
- Testing and analysis of our infrastructure, systems and customer-facing applications.
- Audits of internal and external risks and controls.

Current technology

We utilize up-to-date, industry-standard technology for security, including:

- Industry-accepted encryption to secure data, authentication and digital signatures.
- Enterprise hardware security modules (HSMs) to generate, manage and protect cryptographic keys.
- Network segregation using firewalls, intrusion detections and prevention systems, proxies, data loss prevention, system hardening and multiple levels of malware protection.
- Multi-factor authentication for added account security.

Comprehensive processes

Our security program is aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and includes:

- Penetration testing, code review, system vulnerability, architecture analysis and internal access management.
- Application development that follows DevSecOps best practices.
- Our Vendor Risk Assessment Program to monitor third-party security and risk.
- Regularly updated business continuity, communication and recovery plans in case of cyberattacks.

Cybersecurity is an ongoing, evolving responsibility. We're working on measures to improve security even further, and we look forward to sharing our progress with you in the future. For more information, visit our website and click on Security & fraud at the bottom of any page.

Thank you for your trust in Capital Group.

All Capital Group trademarks mentioned are owned by The Capital Group Companies, Inc., an affiliated company or fund. All other company and product names mentioned are the property of their respective companies.

Capital Client Group, Inc.

© 2024 Capital Group. All rights reserved.