Cybersecurity: TIAA's long-standing practices support DOL's new guidance

In April 2021, the Department of Labor (DOL) published cybersecurity guidelines that provide tips and best practices for retirement plan sponsors, participants and service providers. The DOL's recommendations were issued based on a report from the Government Accountability Office (GAO) titled *Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans*.

TIAA applauds both the GAO and the DOL for thoroughly addressing a topic of such great importance. We have long made cybersecurity and the protection of participant, plan and financial information a top priority, and our current controls and practices are aligned and compliant with the DOL guidelines.

The following are key elements of our cybersecurity program that meet or exceed the GAO/DOL recommendations for service providers.

Information security standards, practices, policies and ongoing compliance

- As a regulated financial institution, TIAA is regularly examined by the Federal Reserve Bank of Boston, the NY Department of Financial Services, the SEC and FINRA, among others.
- In addition to our legal and regulatory obligations, we also map our cybersecurity program against recognized frameworks, such as the International Organization for Standardization/the International Electro-technical Commission (ISO/IEC 27002), the National Institute of Standards and Technology (NIST), and now the DOL, as applicable.
- TIAA is Service Organization Controls (SOC)-certified and is regularly audited by independent parties.
- We maintain a cybersecurity insurance policy.
- TIAA's cybersecurity and fraud programs address fraudulent disbursements and breaches of relevant information systems.
- We operate robust awareness programs to help ensure employees, institutions and participants are aware of cybersecurity risks that they can encounter. These programs are implemented to encourage all to be vigilant and to urge reporting of unusual activity.
- TIAA maintains an incident response team and complies with all existing obligations in respect to breaches, including credit monitoring at its sole expense.
- A detailed Information Security Appendix contained in our contracts with plan sponsors details our obligations around these best practices.

Solutions you can trust

Now more than ever, it is important that strong cybersecurity measures are in place to prevent attacks by criminals taking advantage of a crisis. At TIAA, continually safeguarding the privacy and security of our participants' and client institutions' information is our top priority.

At TIAA, a layered defense protects our clients and participants.

Assess and monitor threats

- 24/7 fraud threat monitoring
- Active participation with key industry threat intelligence groups that share real-time data
- Industry best fraud prevention practices
- Global 24/7 security operations

2B
network events monitored daily

Protect assets

- Multi-factor authentication options
- Mobile app biometric integration
- Voice biometrics
- Encryption of laptops and portable devices
- Patches, antivirus, malware, firewall
- Innovative techniques (artificial intelligence, machine learning, etc.)

14M
network events blocked/reviewed quarterly

Educate our people

- Additional employee education on cybersecurity and awareness during a crisis
- Specialized fraud awareness and training for call center and front-line staff
- Best practices for plan sponsors shared as part of our Cyber Client Engagement Program
- Customer resources for protecting themselves online, including tips to avoid phone scams and phishing

100M
digital logins monitored annually

Our continued commitment to protecting our participants' information

Educating our employees

In partnership with NYU Tandon School of Engineering, TIAA provides employees with the opportunity to obtain a master's degree in cybersecurity. The innovative partnership with NYU Tandon recently earned a CSO50 Award, which recognizes organizations for security projects and initiatives demonstrating outstanding business value and thought leadership.

Customer Protection Policy

At TIAA, our practice is to reinstate a client's TIAA account in full if there is a loss that is determined to be the result of unauthorized activity through no fault of the client. At the same time, we believe it's important that clients take actions to safeguard their account information by following common security practices as outlined at TIAA.org/public/about/inside/topics/security-center/customer-protection-policy.

Find more information on how TIAA protects our participants' information at TIAA.org/public/plansponsors/land/plansponsorcybersecurity.

TIAA

All data as of 12/31/2020.

TIAA-CREF Individual & Institutional Services, LLC, Member FINRA, distributes securities products.

1654902