Transamerica℠

12/25

Constant vigilance and protection

Transamerica's information security program

Transamerica is dedicated to protecting the sensitive information of our customers and partners. Our information security program is continuously updated to address evolving cyberthreats and meet client needs. We also engage independent auditors to provide unbiased assessments of our security controls.

The information security program is an integrated, multifaceted system that works to:

- Safeguard customer information against threats to confidentiality, integrity, or availability
- Prevent unauthorized access to or use of customer information
- Balance protection of customer data and supporting business functionality
- Provide a secure customer experience through proactive controls
- Identify, manage, and oversee remediation of key cybersecurity risks
- Comply with constantly updated regulatory and industry requirements (e.g., federal and state laws, GLBA, SOX, NY DFS, DOL cybersecurity guidelines)
- Supply transformation and technical designs with security in mind

Not for use with plan participants.

We have you protected

Transamerica helps defend your interests in several critical areas of cybersecurity

Governance

- Enable consistent security controls, policies, and standards
- Provide training and workforce education to foster a culture of security
- Reduce third-party information security risk
- Ensure timely and comprehensive response to cybersecurity events
- Employ strategies for business continuity, backup, and recovery

Infrastructure security

- Encryption and monitoring to prevent unauthorized access to the Transamerica network
- Protect against cyberthreats with hardware and workstation protection tools
- Respond to attacks through monitoring, detection, and prevention
- Enhance infrastructure by hardening systems from malicious attacks
- Employ security controls to on-premises and cloud-hosted technologies

Identity management

- Limit access to sensitive data to those with a strict need to know
- Secure the end-user experience through multi-factor authentication, Voice Pass, and automated activity alerts
- Apply additional layered security controls during sensitive online transactions

Application security

- Execute secure coding practices, vulnerability scanning, and penetration testing
- Use application technologies to protect against web threats and evolving attacks
- Employ security features and tools to counter the evolving threat landscape
- Prioritize security through architecture framework

Data protection

- Protect sensitive data while in transit and at rest
- Reduce risk of leakage through data loss prevention (DLP) technologies and processes
- Monitor and protect databases with advanced security tools
- Manage assets to meet and exceed sensitivity, business criticality, and regulatory requirements

Learn more about Transamerica's around-the-clock security

Visit: **transamerica.com/security**

Contact: **Your Transamerica representative**

Not for use with plan participants.

Transamerica℠