CONSTANT VIGILANCE AND PROTECTION

TRANSAMERICA'S INFORMATION SECURITY PROGRAM

Transamerica is committed to safeguarding the sensitive information of our customers and business partners.

Oversight of the Transamerica Information Security Program is a continuous cycle guided by our values, business principles, client needs, and emerging security requirements. We update the program regularly to adapt to the ever-evolving cyberthreat landscape. Additionally, Transamerica engages an independent auditor to assess and provide a clear, unbiased report on the adequacy 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

TRANSAMERICA®

WE HAVE YOU PROTECTED

Transamerica helps to defend your interests in several critical areas of cybersecurity.

GOVERNANCE

- Enable consistent security controls, policies, and standards that support business processes and manage cyber risks
- Provide targeted training and workforce education to foster a security culture and posture
- Reduce third-party information security risk through assessments, governance, and monitoring
- Ensure timely and comprehensive response to cybersecurity events
- Support overall business resiliency management with business continuity, backup, and recovery strategies

INFRASTRUCTURE SECURITY

- Prevent unauthorized access to the Transamerica network through encrypted connections and progressive monitoring capabilities
- Protect against malware and other cyberthreats through hardware and workstation protection tools
- Respond to attacks through next-generation monitoring, detection, and prevention capabilities
- Enhance infrastructure by hardening servers and computers from malicious attacks
- Employ security controls that apply to both on-premises and cloud hosted technologies

IDENTITY MANAGEMENT

- Limit access to sensitive data to only 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
- Implement application technologies to protect against web threats and evolving attacks
- Employ security features and tools to support the ever-changing threat landscape
- Build security during design through our architecture framework

DATA PROTECTION

- Protect sensitive data while in transit and at rest
- Reduce risk of data leakage through data loss prevention (DLP) technologies and processes
- Monitor and protect databases with advanced database 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.

CP3 254351R2 S 10/22

TRANSAMERICA®