TruStage™

Financial Information

Annual Report, Financial Statements, Ratings

TruStage™ financial reports and ratings provide information on the company's financial results and business model. The following information is available in the **Financial Information** section within **About Us** on TruStage's website: **www.trustage.com**

About Us/Financial Information *(click on this link to access the following):*

- Current version of the Annual Report
- Current versions of the Consolidated Financial Statements and Independent Auditor's Report
- Financial ratings for certain entities of TruStage

Frequently Asked Questions

Question	Response
Please provide the most recent Audited Financial Statement with the Opinion for the organization.	The Financial Information page referenced above includes links to the current CUNA Mutual Holding Company Consolidated Financial Statements and Independent Auditor's Report.
Has TruStage had any recent financial audit deficiencies?	Please reference the current Annual Report and/or the CUNA Mutual Holding Company Consolidated Financial Statements and Independent Auditor's Report available on the Financial Information page referenced above.
Does your company have the financial ability to deliver the services and/or goods under the contract? Please provide a copy of the most recent available audited financial statements to identify liquidity, outstanding capital commitments, capital strengths, and operating results.	The Financial Information page referenced above includes links to the CUNA Mutual Holding Company Consolidated Financial Statements and Independent Auditor's Report.
Can you provide A.M. Best Ratings?	The Financial Information page referenced above includes A.M. Best Company's ratings and additional rating agency ratings.

Privacy Policy

The TruStage™ Privacy Policy will help you understand how we collect, use, share and protect personal information we have about you. This Policy applies to CMFG Life Insurance Company, MEMBERS Life Insurance Company, CUNA Brokerage Services, Inc., CUMIS Insurance Society, Inc., Union Security Insurance Company, American Memorial Life Insurance Company, and TruStage Insurance Agency, LLC. The information is available in the **Privacy Policy** section on Trustage's website: **www.trustage.com**

Privacy Policy: *(click on this link to access the following):*

- When this Policy applies
- Types of personal information we collect, where we get it, and why
- Who we share your personal information with, and why
- How your personal information is secured
- Your rights and submitting privacy requests
- And more

Insurance | Investments | Technology

TruStage™

Security Practices

TruStage™ takes our Information Security risk posture very seriously. This document is meant to give an overview of the practices that we follow to protect both our computer systems and the data that has been entrusted to us.

Policies and Procedures

Management has established security policies which are reviewed annually and communicated to all employees. The following general concepts are covered:

- Our security governance framework aligns security strategy with both business objectives and applicable laws and regulations.
- Management will fulfill its responsibilities by designing and implementing business practices based upon industry standards and best practices to protect against unauthorized access, use, disclosure or destruction of corporate information and technology.
- TruStage's position regarding the protection of customer information is derived from several corporate policies that have a bearing on the collection, use and protection of customer data.
- The policies ensure protection of assets not only through documented responsibilities, but also communicated expectations.
- All employees and contractors working on TruStage's behalf are responsible for conducting day-to-day accountabilities in a manner that is consistent with our policies.
- Corporate information and business applications are protected applying administrative, physical and technical safeguards.

Access Control

Access to TruStage's online services and business functions is secured by a unique user ID and password. Passwords must be changed regularly and must adhere to compliance with security policy. Password complexity is set up in order to decrease the risk of unauthorized access to data and business applications. A limited number of administrators have the authority to maintain these policies and set up new user accounts.

TruStage utilizes multi-factor authentication for remote access to our internal networks and for administrative access to our cloud infrastructure. Multi-factor authentication is also available on select TruStage digital properties.

Physical and Environmental Security

All computer hardware and storage media are stored in a limited access facility. Additionally, a copy of all production data and systems resides in a separate, secured facility. These facilities are secured 24-hours per day, 365 days a year, and monitored accordingly. A multi-factor key card system is in place to gain access to the building as well as access to the computer facilities. The key card system logs all activity from the card readers. The system records the card number swiped, date and time and action performed. Access to the computer facilities is limited based on an individual's job responsibilities.

The computer facilities are environmentally controlled. Power is protected by a generator with two independent power feeds. If the generator itself fails, two UPS units provide power to allow for controlled shutdown of equipment. The generator and UPS units are configured to provide as much redundancy in power delivery routes as possible. A separate fire system using dry sprinklers is installed.

Data Encryption

TruStage utilizes data encryption for our online business services that require data transmission. Internally, we have multiple methods to encrypt, mask or tokenize data while in transit and at rest.

Anti-Virus/Malware

TruStage utilizes Endpoint Detection and Response capabilities to scan for viruses and other malicious software. Antivirus software is deployed on our mail service and servers, as well as on all desktops and laptops. Virus signature files are updated as signatures become available. In addition, emergency procedures designed to contain malware outbreaks are in place.

Data Loss Prevention

TruStage utilizes Data Loss Prevention capabilities to assist in preventing unsafe or inappropriate sharing or transferring of sensitive data outside the organization.

Intrusion Detection Capabilities and Firewalls

Intrusion Detection and Prevention systems are in place through which we monitor internal network traffic as well as network traffic to and from the Internet. These systems are designed to detect and block suspicious network traffic. In addition, our segmented networks are also protected by firewalls, proxies, DNS controls and other network security devices and services which further serve to detect, filter and block potentially malicious traffic.

Data Backup and Recovery Procedure

Our procedures require that all production data be backed up on a regularly scheduled basis. The data backup process is automated and monitored for any error situations. Tests are conducted at least annually to ensure critical business processes can be recovered in a timely basis. Tests are also conducted to ensure that the recovery process is correct and that technology platforms and communications between them are operating as intended.

Independent Security Assessments

TruStage employs the services of various external consulting and auditing firms to validate our defenses and report on any findings discovered. In addition, TruStage engages an external firm to perform annual penetration tests.

Incident Response

TruStage has established a formal process for evaluating and responding to security events and potential incidents. A core team from our cross functional areas are available in the event an incident involving our systems is detected. This team is charged with:

- Evaluating the incident
- Determining the appropriate mitigation strategy
- Determining the appropriate notifications to be made which may include law enforcement officials, customers and other third parties

Change Management

TruStage follows best practices for technology change management. The technology change management policy and process incorporate standardized methods and procedures for introducing changes into the production environment in a controlled manner to minimize any change-related service disruptions. The technology change management process utilizes industry best practices such as appropriate chain-of-approval prior to change implementation, oversight and monitoring of the change management process, and clear communications to stakeholders on upcoming changes.

Records Management

TruStage has a formal Records Information Management Program, which is supported by a Records Retention Schedule, as well as departmental procedures. Procedures are in place for storing, retrieving and destroying physical records. TruStage employs a destruction program for all types of documents (paper, fiche, tapes, etc.). Secured bins are provided for paper as well as electronic media for proper disposal.

Third Party Service Providers

TruStage assesses third party service providers' security posture prior to entering into an agreement and on a regular basis throughout the relationship. Security controls and SSAE18 Audit Reports or equivalent are reviewed to ensure their security program follows industry best practices and to identify information security risks and mitigation approaches.

Frequently Asked Questions

Question	Response
Why is some security-related information not shared?	TruStage maintains a layered in-depth security defense. We take the security and confidentiality of our customer data very seriously. Some information may be proprietary and/or sensitive, while other information is not shared to help maintain the integrity and effectiveness of our information security posture. We consider it a best practice to maintain confidentiality regarding our data security practices, safeguards, and procedures. We believe that any other approach increases TruStage's vulnerability to attack.
Does TruStage maintain an internal control framework? Does it align with a particular industry standard?	Yes, we maintain a hybrid internal control framework derived from various sources such as PCI DSS, ISO 27001, NIST 800-53, ITIL, OWASP, CIS, SSAE18 SOC 2 Service Principles and applicable regulations.
How does TruStage ensure its internal control framework remains effective?	Annually, we conduct various internal security risk assessments and engage multiple independent third parties to perform security assessments to ensure our internal security control framework remains effective.

Question	Response
Does TruStage have a security/ incident response plan?	Yes, we have developed a comprehensive Security/Incident Response Plan which is reviewed on no less than an annual basis. (See "Incident Response" in the Security Practices section of the Basic Due Diligence Package.)
Do you provide or make available a formal security awareness training program for all persons with access to customer data?	Formal security awareness training is required annually for the workforce as is data privacy and protection awareness. Various data privacy and security topics are also communicated to the workforce on a regular basis.
Does TruStage maintain a vulnerability and patch management process?	Yes, we actively scan our environment for vulnerabilities, assess vulnerability risks, and patch devices and applications as deemed appropriate.
Do you have anti-malware programs installed on all systems which support on premise and/or cloud service offerings?	Yes, we have anti-malware software installed on all managed devices and systems.
Are security information & event management related logs monitored and retained?	Yes, all pertinent logs are captured and monitored by a third-party service provider. Questionable log events are sent to our Incident Response Team for further analysis.
Are backups maintained off-site?	Yes, backups are maintained off-site.
Does TruStage follow a consistent change management process?	TruStage has a formal Change Management process utilizing industry best practices to ensure changes are implemented into the production environment in a controlled manner.
Does TruStage follow a consistent application development process?	TruStage follows a formal Software Development Lifecycle (SDLC) to ensure applications are developed in a consistent and secure manner across product lines.
What type of process or procedures does TruStage use to detect secure code defects in applications prior to production?	TruStage currently leverages static and dynamic code analysis, peer code reviews as well as vulnerability scans to detect secure code defects.
Do you have controls in place ensuring timely removal of system access which is no longer required for business purposes?	Yes, TruStage has policies and procedures in place for de-provisioning of system access.
Do you utilize encryption to protect data during transport across and between networks, as well as data at rest?	TruStage utilizes industry standard encryption methods to ensure confidentiality of sensitive information. We perform data encryption, masking or tokenization for data at rest and in transit. In addition we use least access privileges to restrict access to need to know.

Question	Response
Does your organization utilize Multi-Factor Authentication?	TruStage utilizes Multi-Factor Authentication for remote access to our internal networks and for administrative access to our cloud infrastructure. Multi-Factor Authentication is also available on select TruStage digital properties.
Do you have documented information security baselines for your infrastructure?	We maintain baseline hardening guides for our infrastructure components.
Do you ensure that security systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry best practices?	Yes, automated features are utilized to ensure security systems remain current or can be deployed real-time as warranted.
Do you have firewalls and network protection in place?	TruStage has multiple firewalls in place, as well as a number of network protection capabilities.
Are passwords required to be changed?	Yes, a robust password policy is maintained for all identities.
Does TruStage have physical security controls for the datacenter?	Yes, we utilize a host of multi-layered security controls to protect the TruStage datacenter.
Are mechanisms in place to detect the presence of unauthorized network devices?	Yes, TruStage has implemented security mechanisms to continuously monitor its network for unauthorized devices.

June 14, 2024
To whom it may concern:

As part of CMFG Life Insurance Company's (TruStage) ongoing commitment to ensuring the security and integrity of its systems and data, TruStage engaged NetSPI to perform a Network Penetration Test; this testing was concluded on May 31, 2024. The purpose of this penetration test was to identify common security issues that could adversely affect the confidentiality, integrity, or availability of TruStage Company systems and data.

NetSPI security consultants follow a phased assessment approach for testing the security of enterprise networks. NetSPI consultants use multiple commercial and open source security tools, custom scripts, and manual techniques to scan for, identify, and exploit vulnerabilities within the systems and devices tested. This methodology identifies an organization's tactical and strategic security challenges by taking a technical snapshot of the current state of security controls. NetSPI security consultants attempt to penetrate or circumvent existing security mechanisms by using software tools and exploit scripts that are similar to those used by attackers. In this manner, our approach analyzes the current security posture and results in recommendations for strengthening security controls.

Sincerely,
Charles Horton
COO

TruStage™

Sourcing and Third-Party Management

This document is intended to outline TruStage's™ sourcing and third-party management practices and controls, including: category management, sourcing and contracting, and third-party management. In addition to extracting value from our third-party relationships and managing costs, our controls have been designed to identify, review, and appropriately manage third-party risks.

Key Terms

The following contains a list of key terms around TruStage's third-party management functions.

- **Enterprise Shared Services** is the department that oversees TruStage's Enterprise Procurement and Third-Party Management functions and policies.
- **Third-Party** is any unaffiliated entity that provides contracted products or services to TruStage, including: Vendors, Legal Firms, Partners, CMFG Ventures Portfolio Companies, Loan Origination System (LOS) / Data Processors, Data Integrators, Credit Union Leagues, Reinsurance Providers, Distributors (e.g. Wholesalers / Broker Dealers), and Referral Providers.
- **Vendor** is any unaffiliated third-party that provides contracted products or services, including:
  - Software (On-Premise, SAAS, PAAS, etc.) Suppliers
  - Hardware and Equipment Suppliers (e.g. IT, IAAS, Telephony, etc.)
  - Professional Services Suppliers (e.g. Consulting Services)
  - Business Process Outsourcing (BPO) Suppliers
  - Marketing, Print, and Postage Suppliers (e.g. Brand, Creative, Print Service Providers, etc.)
  - Contracted Labor Suppliers (e.g. IT, Contingent, etc.)
  - Facility Suppliers (e.g. Janitorial, Landscaping, Furniture, etc.)
  - Third-Party Administrators ("TPAs")
  - Employee Benefits Providers
- **Internal Partners** are representatives of internal corporate functions who participate in (and contribute to) the third-party lifecycle management process, including: identification, onboarding, ongoing monitoring, and offboarding. Internal partners include Sourcing, Third Party Management, Legal Contracting, Data Privacy, Information Security, Human Resources (HR), Finance / Treasury, Information Technology (IT), Governance and Risk Assurance (GRA), Business Partners, and Business Resiliency.

- **Third-Party Engagement Managers (TPEMs)** are TruStage employees who are ultimately responsible for managing the third-party's engagement with TruStage. Specifically, the Third-Party Engagement Manager is responsible for:
  - Understanding TruStage's data privacy and security expectations and requirements when sharing information with third-parties.
  - Partnering with Internal Partners (e.g. IT) to perform the necessary due diligence of potential third-party engagements and ensure a potential third-party meets our organizational policies and controls.
  - Understanding and ensuring that both the third-party and TruStage adhere to the contractual obligations (e.g., payment terms, deliverables review and acceptance, SLAs, etc.)
  - Ensuring TruStage extracts the originally intended business value from the third-party relationship and engagement.
  - Supporting ongoing third-party due diligence and governance efforts.
  - Escalating third-party issues and/or changes to appropriate Internal Partners.
  - Working with a third-party and Internal Partners to address any identified issues and risks.
  - Ensuring the third-party (and its employees) understand and comply with TruStage's applicable corporate policies, including the Third-Party Code of Conduct.

Key Practices and Controls

The following sections outline TruStage's key controls and practices on Sourcing and Third-Party Management.

- **Category Management**

  Enterprise Procurement utilizes category management to build enterprise, third-party strategies to achieve desired value within third-party purchasing areas. Key activities include:
  - Identification and segmentation of third-party purchasing areas or categories (e.g. professional services / consulting).
  - Assemble a cross-functional, enterprise team consisting of key Internal Partners who are major purchasers / consumers within a category.
  - Align on value driver(s) to optimize within category. Value drivers may include: savings, supplier diversity, sustainability, risk mitigation, supply chain resiliency, innovation, etc.
  - Build category management strategies, as well as utilize various procurement levers (e.g. strategic sourcing, strategic relationship management, demand management, etc.) to optimize the category around the defined strategy.
  - Define preferred and approved third-parties.
  - Monitor and update category management strategies, as needed.
- **Sourcing and Contracting**

  Sourcing is a process to evaluate, select, and negotiate with one or more potential third-parties. The sourcing process results in a contractual engagement between TruStage and a third-party. For every

sourcing and contracting activity, EPO assigns a sourcing resource (e.g. buyer or senior buyer) to manage the following key activities:

- Identify and initiate the appropriate sourcing process (e.g. RFx, Contracting, etc.).
- Engage the Third-Party Management Team to facilitate any necessary onboarding (e.g. due diligence) activities.
- In collaboration with Legal, negotiate a contract(s) with a third-party to drive desired outcomes (e.g. advantageous pricing, favorable contract terms, and mitigation of identified risks).
- Ensure contracts contain necessary provisions and terms based upon third-party risk assessment efforts.
- Ensure contracts are reviewed and signed off by appropriate Internal Partners, as well as adhere to Delegation of Authority. Engagements in which an assumed risk exceeds enterprise risk tolerance standards may be escalated through a defined escalation path for further review and appropriate handling.

- **Third-Party Management**

  Third-Party Management is a process to ensure there is a regimented approach for the identification, onboarding, ongoing monitoring, and offboarding of third-parties. The objective of third-party management is to identify and monitor any risks and/or issues, as well as develop plans for remediation. Third-Party Management engages in several key activities including:

  - Assign all third-parties to a **Third-Party Engagement Manager (TPEM)** who is accountable to manage the overall relationship with the third-party and serve as a single point of contact for any third-party questions or requests.
  - Use a risk questionnaire to gather context around the potential third-party engagement, as well as assess inherent risks, including: data privacy, technology and information security, business resiliency, brand / reputational, financial, etc.
  - Engage key Internal Partners based upon the outcome of the risk questionnaire for consultation and/or additional due diligence.
  - Obtain required documentation and information (e.g. SOC2 – Type 2 report) from third-parties to support additional due diligence efforts.
  - Build a third-party ongoing monitoring plan based upon the risk assessment and segmentation. The third-party governance plan will outline the required third-party management activities, as well as the frequency or date of each activity. Third-party management activities may include: review and update of risk questionnaire, conduct business reviews, leverage internal partners to perform additional due diligence, review of certifications and insurance coverages, conduct site visits/audits, perform business resilience planning and/or disaster recovery testing, etc.
  - Partner with the TPEM to ensure required third-party management activities are performed, as well as to provide support and training.
  - Ensure appropriate Internal Partners are engaged in any required third-party management activities, as necessary.
  - Adjust the third-party ongoing monitoring plan and third-party classifications based upon the outcome of third-party management activities, as necessary.

- Collaborate with the TPEM and Internal Partners to develop plans for addressing any risks or issues that may arise from the third-party management activities. Situations in which an assumed risk exceeds enterprise risk tolerance standards may be escalated through a defined escalation path for further review and appropriate handling.
- Utilize industry information and data service providers to proactively monitor some third-party risks and developments (e.g. third-party financial health, bankruptcy filings, merger and acquisition events, liens / judgments, etc.) on a continual basis.

TruStage™

Standard Privacy/Security Terms For Third Party Service Providers

The following is an overview of the standard privacy and security contractual terms for our third-party service providers ("TPSP") that host, store, process or have access to personal information relating to individual customers or prospective customers of TruStage.

Confidentiality and Data Handling Requirements. We impose a number of basic non-disclosure and other confidentiality and security requirements intended to protect personal information and any other confidential or otherwise sensitive data that a TPSP might host, store, process or access in connection with our business/services relationship. These generally include:

- **TruStage Ownership of Data.** As between TruStage and the TPSP, TruStage owns all personal information and other data shared with the TPSP.
- **Confidentiality and Use of Data.** TPSPs must maintain the confidentiality of all personal information and must not use or otherwise disclose any personal information except as required in connection with providing or performing services to or for TruStage.
- **Customer personal information stored in the U.S. only.**
- **Return/Destroy Upon Request or Termination.** TPSPs must return or destroy personal information and other data upon our request or upon termination of our agreement(s).

Compliance with Applicable Data Protection Laws. We require our TPSPs to comply with applicable data protection laws. This includes applicable privacy, data security and cybersecurity laws and regulations.

Notice of Security Incident. We require prompt notice in the event our TPSP becomes aware of or reasonably suspects any unauthorized access to or disclosure, acquisition, or use of personal information.

Information Security Program. We expect our TPSPs to implement and maintain an appropriate information security program that includes reasonable physical, technical and administrative measures to safeguard personal information, including but not limited to written information security policies and procedures, access controls, user identification and password standards, industry standard secure encryption methods to protect the data in transit or at rest, regular vulnerability scans, patch management processes, regular backups and secure logging of all access and changes to personal information.

Security Framework and Independent Security Assessment. We expect our TPSPs to conform to an appropriate security framework and, depending on the nature of the services provided, we may also require an annual or periodic independent security audit (e.g., SOC 2 or other comparable audit).

Coding. For applicable TPSPs, we expect all software and computer code to be designed, developed or configured 1) using secure coding principles and methodologies generally accepted within the computer programming industry; 2) so as not to contain any known vulnerabilities or any embedded viruses, spy ware or other malware; and 3) in compliance with applicable and acceptable Open-Source Software license terms and conditions, where applicable.

Insurance | Investments | Technology

TruStage™

Business Resiliency Disclosure

I. Introduction

TruStage™ is committed to safeguarding business interests during an emergency or significant disruptive event. The company employs an enterprise business resiliency program designed to mitigate risk and provide continuity of operations.

Senior management actively supports the business resiliency program. Dedicated funding and staff are in place to enable actionable and comprehensive business resiliency planning and response.

This disclosure statement to our customers and business partners summarizes the Business Resiliency Program.

Due to proprietary information and privacy concerns the company does not publicly distribute specific program information.

II. Business Resiliency Program Policy

TruStage's corporate policy requires critical business areas to maintain resiliency plans that ensure the enterprise's ability to provide continued insurance and financial products and services to our customers in compliance with applicable laws and regulations. The Business Resiliency Program is responsible for implementation and oversight of this program.

III. Business Resiliency Program Summary

The Business Resiliency Program provides framework, planning, training, exercises, and tools comprising a risk-based resiliency approach to ensure continuous operations.

The program's methodology comprises three main components:

- Prepare
  - Impacts to time-sensitive business capabilities are routinely reviewed and are the basis for determining the recovery priority of these capabilities and associated products. This approach ensures that the recovery of business capabilities is appropriately prioritized to minimize customer impact.
  - Business resiliency plans reside in a secure hosted environment and are regularly exercised, either individually or collectively, using scenarios appropriate to the business functions, department staffs, and facilities. Plans address impacts to people, sites, resources, and technology systems. The program requires that all critical business areas review plans routinely and review if there are changes to business resiliency staffing or business capabilities.
  - TruStage maintains redundant systems and power sources, allowing critical data, telephone systems, and other key elements of our operational infrastructure to be maintained during a regional, local, or facility-related interruption.

- Respond
  - TruStage employs an enterprise-wide Crisis Team to manage the initial response to a disruptive event and to develop strategies for recovery and continuation of operations.
  - Crisis Team members meet with the BR program consultants on a regular basis.
- Recover
  - TruStage will continue to execute resiliency plans until all interrupted business services return to normal operations.

Frequently Asked Questions

Question	Response
Does TruStage have a disaster recovery plan?	Yes. TruStage maintains IT Disaster Recovery plans and conducts regular recovery exercises.
Does TruStage conduct Business Impact Analyses?	Yes. Proprietary information such as when the analyses are performed, and results cannot be provided.
Does TruStage have a pandemic plan?	Yes. The Business Resiliency Program maintains a pandemic plan as part of our crisis response playbook.