Due Diligence Information

TruStage™

CUNA MUTUAL GROUP

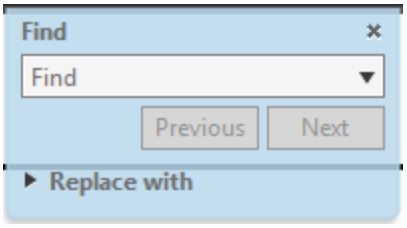
CUNA Mutual Fiduciary Consultants

This information packet is provided to fulfill your credit union's due diligence obligations involving third party relationships.

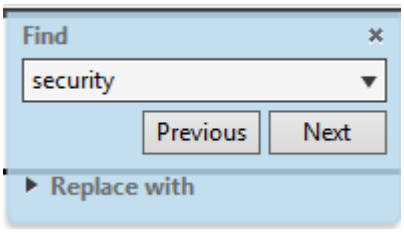
In providing this information, we want to remind you that the information is confidential and proprietary to CUNA Mutual Group. Product or program specific due diligence information may also be attached.

To search this document:

1. Select **Edit** from the menu bar
2. Click **Find** and the **Find** box will display



3. Enter your '**topic'** of interest in the Find field



4. Click **Next, t**he **Find** function will highlight the matches in blue.
5. Navigate through the matches with the **Previous** and **Next** buttons

We trust the attached information will satisfy the fulfillment of your due diligence obligations. If you have any questions, please contact us.

Financial Information

(Annual Report, Financial Statements, Ratings)

CUNA Mutual Group's 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 CUNA Mutual Group's website: www.cunamutual.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 CUNA Mutual Group

Privacy Statement

We understand that you care about how information about you is shared and used, and we appreciate the trust you place with us. At the core of our commitment to protect the people that matter most in your life, is a commitment to protect your privacy in all situations. Our policies and procedures are designed to protect your personal information. This statement describes our commitment to your privacy.

We protect your information. We maintain physical, electronic and procedural safeguards to guard your nonpublic personal information. We restrict employee access to nonpublic personal information about you on an as needed basis.

We do not share your medical information. We do not use or share, internally or with other organizations and third parties, medical information for any purpose other than insurance underwriting or administration of a customer's policy, account or claim, as required by law, or as authorized by you.

We collect relevant information necessary to administer the product or service you have requested and to enhance your experience.

We limit the release of information. We do not sell customer information. We share information only when necessary to administer products and services we provide, when required by law, or when we partner with sponsoring organizations or strategic partners that we believe would be of benefit to you.

We require strict privacy protections in our business relationships. We engage in ventures only with credit unions, organizations and strategic partners that follow strict confidentiality requirements and offer products designed to improve the economic well-being of our customers. When information is released, it is subject to strict privacy protection requirements.

Social Security Number Policy

Social Security numbers are classified as “Restricted” information under our Information Handling Procedure. As such, Social Security numbers may only be accessed by and disclosed when there is a legitimate business “need to know” in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Handling Procedure applicable to Restricted information. These restrictions apply to all Social Security numbers collected or retained by us in connection with customer, employee, or other relationships.

04/24/2019

Online Information Practices

We are committed to protecting your personal privacy as you visit this website. As a visitor to our website, you have the right to understand our privacy and security practices prior to providing the companies of CUNA Mutual Group with personal information.

Information We May Collect

The information we collect varies depending on the type of activity you are performing and helps us personalize and continually improve your experience. Much of our website can be accessed without providing any personal information. On all pages that collect personal information, we specifically indicate what information is required to provide you with the product or service you have requested.

Online Quotes, Applications and Enrollment Forms

When you request a quote, apply online for products or services or provide us information on our website, we may need to collect personal information to complete your request. The personal information we collect varies depending upon the product or service for which you apply. Examples of information we may collect include information such as your name, address, date of birth, gender, employment and financial information, address, e-mail address, Social Security number, beneficiary information, credit card number, etc. Information we capture through applications or enrollments is securely transferred to the corresponding business area for completion.

Employment

We collect personal information such as your name, address, e-mail, and phone number when you apply for employment with us through the website. In addition, we may collect information relating to your employment history when you submit that information as part of an employment application.

Travel and Events

If you register for events or book travel through our website, we will collect personal information from you to complete your request, including your legal name, address, date of birth, travel information, frequent flyer information, phone number, email address, credit card information, and emergency contact information. We securely transmit your registration information to you and to our service providers responsible for booking or coordinating travel or events.

Browsing Information and Technology

We gather information when you visit our website or view/interact with our advertisements or emails. The information we collect may include webpages visited, time of your visit, your IP address, your device ID, operating system, web browser software and performance data, location based on your browser and IP address, referral webpages (such as other websites or an advertisement), actions you take on the website (such as searches you run) and any cookies which were set during a previous visit to our website.

Cookies

A cookie is a small piece of data sent from a website and stored in a file on your browser. A cookie is useful for having the browser remember specific information across several pages or between visits to a website. In addition to cookies, we use scripting, which is code run on

the website to collect information such as actions you've completed on our website or items you click on. We also use pixels, which are transparent images sent from the website to your browser to help us record items like IP address and time. For the purposes of this Privacy Statement, we refer to all these technologies as "cookies."

We do not store any sensitive information within your cookies. Our website does not read any information stored in cookies given to you from other websites, except in rare cases where the other website is a provider of information or functionality within our website and that cookie is necessary to make our website function correctly.

Browsing information is collected to improve your overall experience. We also use the information to track website usage and compile statistics. This helps us improve the website, so you will find it more useful and informative and enable customized promotions you may be interested in. We may use the combination of data we collect, such as browsing information and email address, to join known devices together and provide you personalized experiences on the device you are currently using. Impression data from cookies, which indicates who has seen advertisements about our products and services on our website or third-party websites, may be used to improve our marketing practices. If you are a current customer, have logged into your account, obtain a policy from our website or provide your email address, we may use analytics software to link data we collect, such as use of our website, opening emails we send you or contacting our customer service center via phone, back to you.

We may use browsing information we collect (including IP address, email address and Google Analytics) to match with information received from third parties (including non-personally identifiable behavioral information and device identifiers) and policyholder information as disclosed in our privacy notices to learn more about an individual or a group. These actions help us to analyze interactions with our website, improve marketing efforts, inform our strategic approach and improve the website user's experience. We may also use this information to directly market our products and services, to the extent permitted by law. We may use third parties to perform these and other activities. IP address information is only distributed to third parties when they act as a service provider on our behalf.

You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it. Browsers may also be set up to display a warning when a cookie is used. You may even disable your browser from accepting cookies. Disabling cookies is unique to each device you use. Disabling cookies on one device will restrict the ability to tie that device to other devices you use. Many parts of our website do not function properly if you disable cookies. To provide you with the best possible experience while visiting our website, please enable cookies within your browser.

Cookies can be placed by third party advertising networks. They remember the websites you visit, and that information is shared with other parties, such as advertisers. We may use third-party advertising networks to help us deliver tailored online ads to you.
To learn more about opting-out of this type of interest-based advertising, please visit the Network Advertising Alliance (NAI) Consumer opt-out website.

Do Not Track
Our third-party vendors may collect information about users across our websites. We do not currently have the capability to respond to web browser do not track signals or other mechanisms that provide you with the ability to exercise choice regarding the collection of this information.

Google Analytics
We use a tool called "Google Analytics" to collect information about use of this website. We have implemented the Google Analytics Demographics and Interest Reporting feature. This feature consists of a series of reports where we can see behavior information relating to visitor age, gender and interests. This data can also be used to segment standard reports and create remarketing lists. Visitors can opt-out of Google Analytics for Display Advertising and customize Google Display Network ads using the Ad Settings.

You can opt out of Google Analytics without affecting how you visit the Application. For more information on opting out of being tracked by Google Analytics, visit this Google page.

Mobile Marketing
If you enroll in a CUNA Mutual Group mobile program, you will have the opportunity to opt-in to receive notifications via text message. If you do opt in, we will collect your mobile phone number to send you text notifications. We will send you notifications only according to the terms and conditions of the mobile program you join and will not use the mobile phone number you register with the program for any other purpose without your consent. You may opt-out of receiving these notifications at any time and choosing to do so will not affect your ability to participate in CUNA Mutual Group offerings.

Financial Calculators
We offer online financial management calculators to assist you in your personal financial analysis and planning efforts. The information necessary to perform the calculations includes personal financial information. Where you are logged/signed in to your own secure account, we may store and retain the information you enter to improve your experience and to offer you information about other products and services that may benefit you.

How We Use Your Information
Information collected through this website may be used to:

- Improve the quality of your visits to our website, and your overall experience
- Administer the website and respond to your questions or suggestions
- Fulfill your online application or enrollment requests and otherwise service your transaction
- Personalize your experiences on our website and send offers or information about products and/or services that may interest you
- Learn more about you, including the devices you use to browse our website, and the products or services that may interest you

Who We Share Your Information With

We limit the release of information and we require strict privacy protections in our business relationships. We do not sell customer information. We may share your personal information with our affiliated companies, when required by law, or with third parties that perform functions on our behalf such as:

- Credit unions or strategic partners to offer you a broader array of products and/or services
- Nonaffiliated companies to perform standard business functions

If you prefer that we do not share your personal information for joint marketing purposes with your credit union or any other nonaffiliated financial company, please reply electronically to membersproducts.com/privacychoices or call this toll free-number – **800.834.2617** - to speak to a customer service representative.

Control and Access to Your Information

We enable you to have control over the accuracy of your personal information. You can delete or change your personal account information at any time by contacting us via a method described under “Contact Us” below.

Linking to Third Parties

When you leave this website and go to another linked website, we are not responsible for the content or availability of the linked website. Please be advised that if you enter into a transaction on the third-party website, we do not represent either the third party or you. Further, the privacy and security policies of the linked website may differ from those practiced by us.

Changes to the Privacy Statement

This Privacy Statement was last updated on April 24, 2019. We reserve the right to amend this Statement from time-to-time. Any material change to our online privacy practices will be reflected in this website Privacy Statement. We will indicate the date this Statement was last updated.

Privacy Notices

Privacy notices must be provided when a customer relationship begins and annually thereafter. The notices must be given to members or clients based on the state where the policy or contract was issued. In the case where the policyholder is not the same as the insured or the owner of an annuity and the annuitant are not the same person, the notice should be provided to both parties. Only one notice must be provided per household.

Arizona, Connecticut, Georgia, Massachusetts, Maine, New Jersey, Nevada and Ohio
California
All Other States

International Users

This website is based and administered in the United States of America. The website is governed by the laws of the United States and is not directed at users based outside of the United States.

Contact Us

If you have any questions concerning your privacy, please contact us at:

Mail:
CUNA Mutual Group
P.O. Box 61
Waverly, IA 50677-0061

Telephone:
800.834.2617

Email:
privacychoicesmail@cunamutual.com

If you no longer wish to receive marketing or promotional emails from us, please click the unsubscribe or manage subscriptions link included in the footer of every promotional email we send, or contact us using the options above.

Printer-friendly
Download printer-friendly version of the Privacy Statement

Security Practices

CUNA Mutual Group takes Information Security 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 a security policy which has been communicated to all employees and is reviewed annually. The policy covers the following general concepts:

- Corporate information and business applications are protected applying administrative, physical and technical safeguards.
- Management will fulfill its responsibilities by designing and implementing business practices based upon industry corporate standards to protect against unauthorized access, use, disclosure or destruction of corporate information and technology.
- All employees and independent contractors working on CUNA Mutual Group's behalf are responsible for conducting day-to-day accountabilities in a manner that is consistent with this policy.

Access Control and Business Resiliency
Access to CUNA Mutual Group'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 setup new user accounts.

All computer hardware and storage media is 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. These logs are reviewed periodically by Computer Operations management. 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. Separate smoke detectors are also installed. Air handlers have adequate dust filtering systems and static electricity is controlled by maintaining a humidity level of 45%. All moving devices are enclosed to protect them from exposure to elements. (Please see Business Resiliency Disclosure in this Due Diligence packet for policies and procedures.)

Data Encryption
CUNA Mutual Group 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 Software
CUNA Mutual Group utilizes End Point Protection which scans for viruses and other malicious software. Antivirus software has been deployed on our mail service and servers, as well as on all desktops and laptops. IT updates virus "signature" files as signatures become available. In addition, emergency procedures designed to contain malware outbreaks are in place.

Data Loss Prevention Software
CUNA Mutual Group utilizes Data Loss Prevention capabilities to ensure sensitive data does not leave the corporate network.

Intrusion Detection Capabilities and Firewalls
Intrusion Detection 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 suspicious network traffic. In addition, our segmented networks are also protected by firewalls, proxies and other network devices which further serve to filter and block suspicious traffic that is detected.

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. A large-scale recovery test is performed annually. The annual tests are conducted to ensure each critical business process can be recovered in a timely basis. The test is also conducted so that we can attempt to ensure that the recovery process is correct and that all the technology platforms and communications between each are operating as we intend.

Independent Security Assessments
CUNA Mutual Group employs the services of various external consulting and auditing firms to validate our defenses and report on any findings discovered. In addition, CUNA Mutual Group obtains a statement of opinion regarding our penetration tests annually.

CUNA Mutual Group'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. Our security governance framework aligns security strategy with both business objectives and applicable laws and regulations. The policies ensure protection of assets not only through documented responsibilities, but also communicated expectations.

Incident Response
CUNA Mutual Group 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
CUNA Mutual Group follows best practices for technology change management. The technology change management policy and process incorporate standardized methods and procedures for introducing changes into the IT 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
CUNA Mutual Group is very concerned about appropriately protecting customer information and other corporate records. We have a formal Records Information Management Program, which is supported by a Records Retention Schedule, as well as departmental procedures. We also have procedures for storing, retrieving and destroying physical records. CUNA Mutual Group employs a total shredding program for all paper documents. Secured bins are provided for paper as well as electronic media for proper disposal.

Third Party Vendors
CUNA Mutual Group assesses all vendors and reviews their SSAE18 Audit Reports to ensure they follow best practices. Where necessary, ongoing assessments continue to occur on a regular basis.

800 Washington Ave N Suite 670
Minneapolis, MN 55401
888.270.0317

Monday, October 22, 2018

As part of CUNA Mutual Group's (CUNA) ongoing commitment to ensuring the security and integrity of its systems and data, CUNA engaged NetSPI to perform an internal and external network penetration test, this testing completed in September 2018. The purpose of the penetration tests was to identify common security issues that could adversely affect the confidentiality, integrity, or availability of CUNA 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 like those used by attackers. In this manner, our approach analyzes the current security posture and results in recommendations for strengthening security controls.

CUNA Mutual Group has shown a great awareness of their security posture, which has resulted in a security program that NetSPI believes is mature for their industry. CUNA Mutual Group is in the process of remediating the issues discovered during the assessments in order of potential risk to the organization.

Sincerely,

Charles Horton
SVP of Services

Sourcing and Vendor Management

Functional Policy

To Whom this Policy Applies

This policy applies to all employees, contractors, and members of boards of directors of member companies of CUNA Mutual Group and non-employees, including agents and business partners.

Purpose of this Policy

This policy aims to establish a company-wide framework designed to identify, review and appropriately mitigate Vendor risks, control costs and maximize value of the Sourcing and Vendor Management Office's (SVMO) Vendor relationships throughout the Contract Lifecycle.

Key Terms to Understand

- **Vendor** is any unaffiliated entity that provides any contracted good or service in return for payment or other remuneration (including potential future revenue – e.g., proof-of-concepts or pilots). Entities engaged with CUNA Mutual Group in partnerships, joint ventures, marketing relationships or value-added services may be included.
- **Sourcing** is a process to evaluate and select one or more potential Vendors, resulting in a contract between the Company and selected Vendor(s).
- **Vendor Management** is a process to govern existing Vendors through the contract lifecycle in order to ensure a regimented review of identified risks and to monitor and improve performance.
- **Stakeholders** are internal corporate functions which contribute to the risk identification, review and mitigation, cost control and value maximization of Vendors in partnership with the SVMO.
- A **Managed Vendor** is a Vendor whose relationship with the organization has risk, operational or performance implications of significance to require a Vendor Management Plan.
- **Contract Lifecyle** describes the processes involved with a Vendor from contract execution, rendered services, payments, Vendor Management, termination and transition of services where applicable.

What this Policy Requires*

This policy governs all Vendor interactions. The SVMO is required to participate in Sourcing transactions and ongoing Vendor Management monitoring.

The SVMO, Legal and all Stakeholders shall be responsible for the following procedures: Governance and Risk Management, Sourcing, Vendor Management and Contract Management. All employees who engage or manage Vendors must be familiar with these procedures.

Governance and Risk Management

- All Vendors under contract must be evaluated by the SVMO to determine their relationship type. The SVMO will measure each Vendor's risk level and their importance and combine them to form a relationship type. The SVMO will govern processes related to risk assessment, performance management, contract compliance and regulatory / policy compliance for all Vendors in accordance with their relationship type.

Sourcing

All transactions with Vendors must be evaluated by the SVMO to determine the Vendor's potential relationship type. For every Sourcing transaction, the SVMO will:

- Identify risks, quantify risks as needed, and provide risk mitigation recommendations in conjunction with Legal and other due diligence partners.
- Be responsible for Stakeholder participation
- Define a Sourcing Process appropriate to the engagement
- Create a summary of risks and material elements of the contract for those Stakeholders impacted by the transaction.

- All Vendor transactions must involve the SVMO. All transactions with Vendors require a written contract, along with the relevant business function(s), and require sign-off by other Stakeholders as appropriate.

Contracting
All contracts must be compliant with the President's Delegation of Authority Policy.

Vendor Management
- The SVMO will oversee and provide guidance for the Vendor Management of all active managed Vendors. Each business area's assigned SVMO Customer Lead will partner with business executives and Stakeholders to execute projects or develop strategic recommendations which affect the Vendor ecosystem.
- Employees must work with the SVMO to produce signed documents (by the officer responsible for the SVMO) showing those Vendors which are considered Third Party Administrators by state regulatory agencies are actively administered by the SVMO.
- All vendor relationship managers should ensure that the active Vendors they are responsible for understand and comply with applicable corporate policies, including the Code of Supplier Conduct.

Contract Administration
- All signed contracts that authorize monetary transactions must document the Vendor's expected payment stream.
- The SVMO will work with Finance to determine the most efficient payment mechanism.
- All contractors that require system access or building access via a security badge must be set up in the Vendor Management System and should be paid through this system. Exceptions may be made only by the Director of Procurement.

Supplier Diversity
- All sourcing selection efforts must ensure fair and impartial consideration is given to each DOBE (Diversely-Owned Business Enterprise) and the products/services they provide. The selection criteria must ensure that purchases made from DOBEs are made solely on the basis of quality, delivery, price and acceptable terms and conditions.

**** Please note: If there is any conflict between terms of this Functional Policy and a related Corporate Policy, the terms in the Corporate Policy will control. Violations of this policy may result in discipline up to and including termination of employment.***

Business Resiliency Disclosure

I. Introduction

CUNA Mutual Group is committed to safeguarding business interests in the event of an emergency or significant disruption of business operations. This is accomplished through a dynamic enterprise business resiliency program designed to 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 our Business Resiliency Program. Proprietary information and privacy concerns do not allow specific program information to be publicly distributed.

II. Business Resiliency Program Policy

CUNA Mutual Group corporate policy requires 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 Department is responsible for implementing this program.

III. Business Resiliency Program Summary

The Business Resiliency Program provides the framework, planning, training, exercises, and tools to enable a risk-based approach to resiliency which addresses both geographical and/or operational interruptions. Our program's methodology has three main components:

- Prepare
  - The Business Resiliency department conducts a regular Business Interruption Impact Analysis (BIIA) for all products and associated business capabilities. 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 for the business functions or facility. Plans cover interruptions to people, workspaces, suppliers, and technology.
  - Prevention is also a hallmark of business resiliency. For example, specific to pandemic planning, we conduct regular employee safety and hygiene awareness campaigns, monitor health organizations' trends, and review internal absentee rates.
  - CUNA Mutual Group maintains redundant systems and power sources, allowing critical data, telephony, and other facility-dependent operations to be maintained during a regional or local interruption. In the event it is not possible to conduct business from a CUNA Mutual Group office, alternate company resources and/or contracted external recovery service vendors support resiliency of our most time-sensitive business capabilities.
- Respond
  - Business Resiliency Response teams are in place at all major CUNA Mutual Group locations. They address the management of initial response and the strategies for recovery and continuation of operations. Team members are trained; their plans and duties are reviewed and exercised annually.
- Recover
  - Resiliency plans are executed until all interrupted business services are returned to normal operations.

Due Diligence

Frequently Asked Questions

Question	Response
Financial	
Please provide current annual report or financials for past two years.	See the Financial Reports page of the Due Diligence packet which includes a link to the Financial Information page on CUNA Mutual Group's web site (cunamutual.com).
Please provide the most recent Audited Financial Statement with the Opinion for the organization.	See the Financial Reports page of the Due Diligence packet which includes a link to the Financial Information page on CUNA Mutual Group's web site (cunamutual.com). The Financial Information page includes links to the Consolidated Financial Statements and Independent Auditor's Report.
Has CUNA Mutual Group had any recent financial audit deficiencies?	See the Financial Reports page of the Due Diligence packet which includes a link to the Financial Information page on CUNA Mutual Group's web site (cunamutual.com). The Financial Information page includes links to the Consolidated Financial Statements and Independent Auditor's Report.
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.	See the Financial Reports page of the Due Diligence packet which includes a link to the Financial Information page on CUNA Mutual Group's web site (cunamutual.com). The Financial Information page includes links to the Consolidated Financial Statements and Independent Auditor's Report.
Can you provide A.M. Best Ratings?	See the Financial Reports page of the Due Diligence packet which includes links to the Financial Information page on CUNA Mutual Group's website (cunamutual.com). Under the heading Financial Ratings are the A.M. Best Company's ratings and additional rating agency ratings.
Information Security	
Why is some security-related information not shared?	CMFG Life 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 CUNA Mutual Group's vulnerability to attack.
Do you have anti-malware programs installed on all systems which support your on premise and/or cloud service offerings?	Yes, we have anti-malware software installed on all managed devices and systems.

Question	Response
Are logs monitored and retained?	Yes, all pertinent logs are captured and monitored by a third-party service provider. Questionable logs events are sent to our Incident Response Team for further analysis.
Are backups maintained off-site?	Yes, backups are maintained off-site.
Does CUNA Mutual Group follow a consistent change management process?	CUNA Mutual Group has a formal Change Management process utilizing industry best practices to ensure changes are implemented into the production environment in a controlled manner.
Does CUNA Mutual Group follow a consistent application development process?	CUNA Mutual Group 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 CUNA Mutual Group use to detect secure code defects in applications prior to production?	CUNA Mutual Group currently leverages static and dynamic code analysis, peer code reviews as well as vulnerability scans to detect secure code defects.
Does CUNA Mutual Group maintain a security internal control framework? Does it align with a particular industry standard?	Yes, we maintain a hybrid internal control framework derived from various security frameworks such as COBIT 5, PCI DSS, ISO 27001, NIST 800-53, and SSAE18 Service Organization Controls guidelines.
Is all data hosted in the United States?	Yes, our hosted/cloud services providers currently maintain all data within the United States.
Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes, CUNA Mutual Group has policies and procedures in place for de-provisioning of systems access.
Do you utilize encryption to protect data during transport across and between networks, as well as data at rest?	CUNA Mutual Group 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 and use least access privileges to restrict access to need to know.
Does your organization utilize Multi-Factor Authentication?	CUNA Mutual Group utilizes Multi-Factor Authentication for remote access to our internal networks. Multi-Factor Authentication is also available on select CUNA Mutual Group 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.
Does CUNA Mutual Group 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 Due Diligence Packet.)
How does CUNA Mutual Group 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. Examples of our control framework reviews include: • SSAE 18 SOC 1 – Pensions/Retirement Services • SSAE 18 SOC 2 – Lending, CBSI and TruStage Reports and/or statements of opinion are available to our customers through our Due Diligence Center.

Question	Response
Do you have firewalls and network protection in place?	CUNA Mutual Group has multiple firewalls in place, as well as a number of network protection capabilities.
Are passwords required to be changed?	CUNA Mutual Group maintains a robust password policy for all identities.
Does CUNA Mutual Group have physical security controls for the datacenter?	Yes, we utilize a host of multi-layered security controls to protect the CUNA Mutual Group datacenter.
Are mechanisms in place to detect the presence of unauthorized network devices?	Yes, CUNA Mutual Group has implemented security mechanisms to continuously monitor its network for unauthorized devices.
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 provided annually as are general awareness communications on various data privacy and security topics.
Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes, CUNA Mutual Group has established procedures in place for approval, download and installation of software.
Does CUNA Mutual Group 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.
Business Continuity	
Does CUNA Mutual Group have a disaster recovery plan?	Yes, see the Business Resiliency Disclosure section in the Due Diligence packet.
Has a Business Impact Analysis been performed?	Yes, see the Business Resiliency Disclosure section in the Due Diligence packet. Note: Business Impact Analyses for all business functions are regularly conducted. Proprietary information such as when the analyses are performed and results cannot be provided.

TruStage Insurance Program Privacy FAQs

Introduction

Protecting member privacy is a priority for the insurance companies of the CUNA Mutual Group. Our physical, electronic, and procedural safeguards combine to protect nonpublic personal information in accordance with applicable federal and state laws and regulations. Through cooperative efforts between credit unions and the TruStage Insurance Program, credit unions can protect their members' privacy and maintain compliance with all applicable laws and regulations.

1. **Under the TruStage Insurance Program is it permissible for credit unions to share membership information with CUNA Mutual Group?**

   Yes, as long as the credit union follows the requirements set forth in the National Credit Union Association Consumer Privacy Rule, 12 C.F.R. Part 716 (NCUA §716). This Rule allows sharing of nonpublic personal information to nonaffiliated third parties as long as (1) the credit union provides their members with a privacy notice that contains language stating they disclose information to third parties; and (2) there is a contractual agreement between the parties that prohibits disclosing or using the information other than to carry out the purpose for which the information is disclosed.

2. **Do credit unions have to offer an 'opt out' to members at the time they send out their privacy notice?**

   As long as the credit union provides the privacy notice and meets the contractual obligations of NCUA §716, no opt out is required to be provided to the members. (Some state variations may apply) (See, NCUA §716.13(a)(1), FTC §313.13(a)(1) CUNA Mutual Group's TruStage Insurance Program includes a Joint Marketing Agreement between the credit union and CUNA Mutual Group that includes a provision that requires the parties to protect members' nonpublic personal information. **Credit unions should check with their legal counsel to determine if there are any state variations that may require an opt-out.**

3. **Do the same requirements apply if the member requests a service or initiates a transaction?**

   The requirements of the initial notice and opt out do not apply if the credit union discloses nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with any of the following:

   - Servicing or processing a financial product or service that a consumer requests or authorizes.
   - Maintaining or servicing the consumer's account with the credit union, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity.
   - A proposed or actual securitization, secondary market sale (including servicing rights) or similar transaction related to a transaction of the consumer. (See, NCUA §716.14, FTC §313.14)

4. **Are credit unions an affiliate of CUNA Mutual Group?**

   No. The insurance companies of the CUNA Mutual Group are separate entities that may engage in joint marketing with credit unions. CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates.

5. **Does the Gramm-Leach-Bliley Act (GLBA) prohibit financial institutions from sharing information such as Social Security numbers and date of birth with nonaffiliated third parties?**

   In general, as long as credit unions notify members in their privacy notices that they share nonpublic personal information, credit unions can share this information under GLBA requirements. Nonpublic personal information is broad and includes any personal information the credit union obtains through the course of doing business with the member. For most member information sharing activities, it typically includes the person's name, address, Social Security number, birth date and telephone number. Also included is member relationship information in a credit union such as effective dates, termination dates, product codes (Share Savings, Share Draft, etc…). For more information See, NCUA §716.3 & §716.6.

   Keep in mind apart from GLBA, information sharing requirements do vary at the state level. There may be state laws in place that prohibit sharing certain types of data.

6. **What impact does the federal model privacy notice have?**

   In late 2009, the National Credit Union Administration and seven other federal agencies (Agencies) released a final model privacy notice form (Federal form). The previous rules permitted financial institutions to use model language (called Sample Clauses) in their privacy notices. The Federal form is designed to replace the Sample Clauses and make it easier for consumers to understand how financial institutions collect and share their personal information. The Federal form is intended to simplify privacy notices for consumers and create uniformity for comparison purposes. **Credit unions should check with their legal counsel to determine if there are any state variations that would affect the credit union's ability to use the federal model privacy notice.**

7. **What assistance will CUNA Mutual Group provide to credit unions with their privacy notice obligations?**

   CUNA Mutual Group's LOANLINER® Deposit Documents can assist your credit union in creating a tailored Privacy Disclosure that may be provided with other disclosures during the membership/account opening process. The disclosure may also be used to fulfill annual notice requirements by inserting it with quarterly or monthly statements for ease of distribution to members. You may initiate an order for the LOANLINER® Privacy Disclosure by completing and submitting the Privacy Disclosure Order Request and Questionnaire. You may obtain the Order Request and Questionnaire by calling 800.356.5012 (option #1) or by visiting www.loanliner.com (click '*LOANLINER Compliance Solutions'* on the left-hand side of the page; then submit an inquiry).

8. **With the amendment to the GLBA annual privacy notice requirement, credit unions no longer need to send an annual privacy notice as long as they meet certain conditions, including not sharing information with nonaffiliated third parties. How does this affect our sharing practices under the TruStage Insurance Program?**

   The Fixing America's Surface Transportation (FAST) Act became effective in December, 2015. It contains a privacy notice provision based on the Eliminate Privacy Notice Confusion Act. The provision amends the Gramm-Leach-Bliley Act (GLBA) annual privacy notification requirements.

The 2015 GLBA amendment eliminates the annual privacy policy notice requirement for an institution that does not share information with nonaffiliated third parties (and extends to those that share through some exceptions) and does not change its privacy policy from the last time it was disclosed.

In August of 2018, the Bureau of Consumer Financial Protection (aka CFPB) finalized a privacy rule implementing the 2015 GLBA amendment. The privacy rule clarifies that if the financial institution meets the exceptions to not provide the annual privacy notice, they no longer must use the “alternative method” of posting a privacy notice on the website for annual purposes (however, there is no penalty for continuing that practice). Initial privacy notice requirements are not impacted by the 2015 GLBA amendment nor the 2018 implementing privacy rule.

Both the GLBA amendment and the CFPB rule generally apply to federally chartered credit unions that share member data with nonaffiliated third parties under certain exceptions, which includes sharing nonpublic personal information to perform services for or functions on behalf of the financial institution and marketing of the financial institution's own products or services, **or financial products or services offered pursuant to joint agreements between two or more financial institutions**. The financial institution must fully disclose the providing of such information and also enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information. Our TruStage program falls under the joint marketing exception. An exception also exists for sharing to service providers, law enforcement, or as necessary to fulfill a transaction requested by the customer.

Credit unions should ensure they understand any state laws that continue to require the annual privacy notice.

03/2019

Liberty Mutual Due Diligence

The TruStage Auto & Home Insurance Partner Management Team conducts regular reviews with our strategic partners and their technology security practices.

- CUNA Mutual Group takes security related to external strategic partnerships seriously. To that end, audits with strategic partners take place on a regular basis and include SSAE 16 reporting, compliance with Gramm-Leach-Bliley Act (GLB), and statements of security and privacy practices. These reviews take place as part of the selection process, before ever doing business with a strategic partner, and then on a regular basis, annually if appropriate.
    - Data security:
        - Our partners have computer security procedures in place to protect all personal information of their policyholders.
        - Our partners ensure physical security measures are in place to control physical access to systems or outputs that contain personal data and privileged information.
        - Only necessary information is gathered and stored for only as long as it is needed; when it is no longer needed it is properly disposed of in a safe and secure manner.
    - Data privacy:
        - Our partners have privacy practices and controls in place that are in full compliance with state insurance codes and all applicable regulatory requirements.
        - Our partners are limited in the data they share back with CUNA Mutual Group. For example, we only receive data that is necessary to maintain business processes.
- Annual reports are available at Liberty Mutual

REVISED: April 30, 2018

Esurance Due Diligence

The TruStage Auto & Home Insurance Partner Management Team conducts regular reviews with our strategic partners and their technology security practices.

- CUNA Mutual Group takes security related to external strategic partnerships seriously. To that end, audits with strategic partners take place on a regular basis and include SSAE 16 reporting, compliance with Gramm-Leach-Bliley Act (GLB), and statements of security and privacy practices. These reviews take place as part of the selection process, before ever doing business with a strategic partner, and then on a regular basis, annually if appropriate.
    - Data security:
        - Our partners have computer security procedures in place to protect all personal information of their policyholders.
        - Our partners ensure physical security measures are in place to control physical access to systems or outputs that contain personal data and privileged information.
        - Only necessary information is gathered and stored for only as long as it is needed; when it is no longer needed it is properly disposed of in a safe and secure manner.
    - Data privacy:
        - Our partners have privacy practices and controls in place that are in full compliance with state insurance codes and all applicable regulatory requirements.
        - Our partners are limited in the data they share back with CUNA Mutual Group. For example, we only receive data that is necessary to maintain business processes.
- Annual reports are available via Allstate (Esurance's Parent Company)

REVISED: February 12, 2019

GoHealth Due Diligence

The TruStage Auto & Home Insurance Partner Management Team conducts regular reviews with our strategic partners and their technology security practices.

- CUNA Mutual Group takes security related to external strategic partnerships seriously. To that end, audits with strategic partners take place on a regular basis and include SSAE 16 reporting, compliance with Gramm-Leach-Bliley Act (GLB), and statements of security and privacy practices. These reviews take place as part of the selection process, before ever doing business with a strategic partner, and then on a regular basis, annually if appropriate.
    - Data security:
        - Our partners have computer security procedures in place to protect all personal information of their policyholders.
        - Our partners ensure physical security measures are in place to control physical access to systems or outputs that contain personal data and privileged information.
        - Only necessary information is gathered and stored for only as long as it is needed; when it is no longer needed it is properly disposed of in a safe and secure manner.
    - Data privacy:
        - Our partners have privacy practices and controls in place that are in full compliance with state insurance codes and all applicable regulatory requirements.
        - Our partners are limited in the data they share back with CUNA Mutual Group. For example, we only receive data that is necessary to maintain business processes.
- To learn more about GoHealth, go to www.gohealthinsurance.com/about-us

REVISED: February 12, 2019