Due Diligence Information

TruStage™

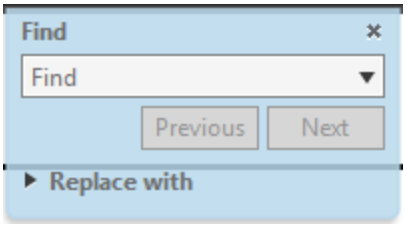
CUNA MUTUAL GROUP
CUNA Mutual Fiduciary Consultants

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

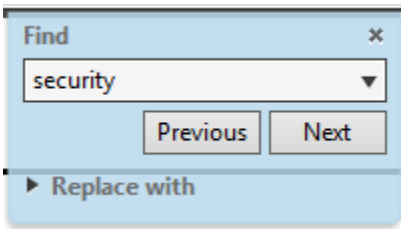
In providing this information, we want to remind you that the information is confidential and proprietary to CUNA Mutual Group. Product or program specific due diligence information may also be attached.

This Document is Easy to Search!

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.

Annual Financial Reports

CUNA Mutual Group's 2017 financial reports provide information on the company's financial results and business model. The following information is available in the About Us section on CUNA Mutual Group's website: www.cunamutual.com

- Online Annual Report or a printable Annual Report
- Consolidated Financial Statements and Independent Auditor's Report is available under About Us/Financial Information
- Financial ratings for certain entities of CUNA Mutual Group are available under About Us/Financial Information, see heading Financial Ratings

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.

Online Information Practices

We are committed to protecting your personal privacy as you visit this website. As a visitor to our site, 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 in order to provide you with the product or service you have requested.

Online Applications and Enrollment Forms

When you apply online for products or services, we may need to collect personal information in order 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, email 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.

Browsing

When you visit our site, we gather information including page requests (URL requests), time of your visit, your IP address, operating system, web browser software, and any cookies which were set during a previous visit to our site. This information is collected to improve your overall experience. We also use the information to track site usage and compile statistics. This helps us improve the site so that you will find it more useful and informative and enable customized promotions you may be interested in. IP address information is not distributed to third parties.

Google Analytics

We use a tool called “Google Analytics” to collect information about use of this site. 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.

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 site, and your overall experience
- Respond to your questions or suggestions
- Fulfill your online application or enrollment requests and otherwise service your transaction
- Send offers or information about products and/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 in order to perform standard business functions on our behalf.

If you prefer that we do not share your personal information for marketing purposes with your credit union or any other nonaffiliated third party, please reply electronically to members.cunamutual.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 account information. You can delete or change your personal account information at any time by contacting us via a method described under “Contact Us” below.

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.

Cookies

A cookie is a file containing data that a website can send to your browser, which is then stored on your system. A cookie is useful for having the browser remember specific information across several pages or between visits to a website. We do not store any sensitive information within your cookie. Also, our site 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.

Our website makes use of cookies for the following purposes:

- Website administration and personalization
- Completing your request
- Analysis of page and website information that does not identify specific individuals

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. In order to provide you with the best possible experience while visiting our website, please enable cookies within your browser. Many parts of our site do not function properly if you disable cookies.

Linking To Third Parties

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

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

Changes To The Privacy Statement

This Privacy Statement was last updated on April 26, 2017. 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.

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

Security Practices

CUNA Mutual Group takes Information Security very seriously. This document is meant to give an overview of the practices that we follow in order 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 with CCTV cameras. 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. Access is reviewed at least semi-annually by Computer Operations management.

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 for policies and procedures.)

Data Encryption
CUNA Mutual Group supports Transport Layer Security (TLS) and Secure Socket Layer (SSL) data encryption for our online business services that require data transmission. Secure FTP and TLS can be utilized for transmitting data securely to and from third parties. 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 an End Point Protection tool, which scans all files for viruses and other malicious software. Antivirus software has been deployed on our mail and web servers, as well as on all desktops and laptops. IT updates virus "signature" files on a weekly basis or as signatures become available during crisis. In addition, emergency procedures designed to contain any virus outbreaks are in place.

Data Loss Prevention Software
CUNA Mutual Group utilizes a Data Loss Prevention tool 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 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 backups are done centrally. 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 in an attempt 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 of 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 test 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 a number of 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 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 incorporates 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 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 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 SSAE16 Audit Reports to ensure they follow best practices. Where necessary, ongoing assessments continue to occur on a regular basis.

CUNA MUTUAL GROUP
INSURANCE • SERVICES • ASSET MANAGEMENT

May 3, 2017

CUNA Mutual Group has a robust Corporate Security and Safety program which is designed to protect Credit Union Member data as well CUNA Mutual data, facilities and personnel. A vended DDoS defense system is provided by our primary internet service provider. We also maintain an automated Intrusion Detection System. These defense mechanisms block and remove malicious traffic before it has an opportunity to adversely reach and/or affect our network. In addition, we utilize an End Point Protection tool which scans all files coming into our network for viruses and other malicious software. Antivirus software has been deployed on our mail and web servers, desktops and laptops. IT updates virus "signature" files multiple times a day. In addition, emergency procedures designed to contain any virus outbreaks are in place per our Incident Response and Business Resiliency Programs. Backups and replication are performed for critical infrastructure and can be restored to the state prior to a ransomware or crypto-locker compromise.

CUNA Mutual Group corporate policy requires business areas to maintain resiliency plans that ensure the enterprise's ability to provide continued insurance, financial products and services to our customers in compliance with service level agreements. 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. The Crisis Communications Team works with respective business owners and establishes and maintains clear, accurate, and timely communications with CUNA Mutual Group employees, customers, providers, and regulators.

If you have any additional questions, please contact me at (608) 665-7634.

Sincerely,

Lisa Lybeck
Chief Information Security Officer | Information Technology
CUNA Mutual Group
800.356.2644, Ext: 665.7634

Sourcing & Vendor Management Policy

APPLIES TO ALL EMPLOYEES AND NON-EMPLOYEES (e.g., AGENTS, CONTRACTORS, GUESTS AND BUSINESS PARTNERS)

PURPOSE

To establish a company-wide framework designed to ensure Vendor risks are mitigated, costs controlled and value maximized.

DEFINITIONS

Third Party Vendor ("Vendor") is any unaffiliated entity that provides any contracted good or service in return for payment or other remuneration. Entities engaged with CMFG Life in partnerships, joint ventures and marketing relationships 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 Vendors.

Vendor Management is a process to govern existing Vendors through the contract lifecycle in order to mitigate identified risks and to monitor and improve performance.

Stakeholders are internal corporate functions which contribute to the risk mitigation, cost control and value maximization of Vendors in partnership with the SVMO.

REQUIREMENTS

The Sourcing and Vendor Management Office ("SVMO") evaluates, governs and monitors all Vendor relationships and transactions to maximize supply base value while managing risk.

This policy governs all Third Party Vendor interactions except:

1. The provision of legal services by the Legal Department.
2. The provision of audit services for the review of corporate financial statements and accounts.
3. The hiring of confidential investigative services by Legal, Internal Audit, or Security.
4. The acquisition, divestiture, lease or disposal of real property.
5. Corporate finance, investment, insurance and re-insurance transactions.
6. Mergers, acquisitions, and divestiture transactions.
7. Customer contracts.
8. Other transactions authorized by the Officer responsible for the SVMO or the Chief Legal Officer.

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 Third Party Vendors must be familiar with these procedures.

Governance and Risk Management

All Third Party Vendors under contract must be evaluated by the SVMO to determine their relationship type to CMFG Life. 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, contract compliance and regulatory / policy compliance for all Vendors in accordance with their relationship type.

Sourcing
All transactions with Third Party 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 the risks and material elements of the contract for those Stakeholders impacted by the transaction.

All transactions must involve the SVMO. All transactions with Third Party Vendors require a written contract that is approved by the SVMO and Legal, along with the relevant business function. 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 actively 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 must ensure that the active Vendors they are responsible for comply with 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 consultants 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 the SVMO.

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.

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 2016 Financial Reports page of the packet to link to CUNA Mutual Group's web site (cunamutual.com)
Please provide the most recent Audited Financial Statement with the Opinion for the organization.	See the 2016 Financial Reports page of the packet to link to CUNA Mutual Group's web site (cunamutual.com) or the links to the Consolidated Financial Statements and Independent Auditor's Report on CUNA Mutual Group's web site.
Has CUNA Mutual Group had any recent financial audit deficiencies?	See the 2016 Financial Reports page of the packet to link to CUNA Mutual Group's web site (cunamutual.com) or the links to the Consolidated Financial Statements and Independent Auditor's Report on CUNA Mutual Group's web site.
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 2016 Financial Reports page of the packet to link to CUNA Mutual Group's web site (cunamutual.com) or the links to the Consolidated Financial Statements and Independent Auditor's Report on CUNA Mutual Group's web site.
Can you provide A.M. Best Ratings?	See the 2016 Financial Reports page in the packet to a link to CUNA Mutual Group's website and go to the Financial Information page and under Financial Ratings is the A.M. Best Company's 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?	CUNA Mutual Group scans all files coming into its network for viruses and other malicious software. Anti-virus software has been deployed on our mail, application and database services, as well as on all desktops and laptops. We also use spam filtering and device encryption. Incident response procedures have been developed if there is a need to contain any virus outbreaks should they arise.
Are logs monitored and retained?	Yes, all pertinent logs are captured and monitored by a third-party logging vendor 24/7/365. Questionable logs events are sent to our Incident Response Team for further analysis.
Are backups maintained off-site?	Yes, backups are maintained off-site.

Question	Response
Does CUNA Mutual Group follow a consistent application development and change management process?	Utilizing industry best practices, CUNA Mutual Group has a formal SDLC and Project Management Methodology to ensure changes are implemented into the production environment in a controlled manner.
Do you utilize an automated source-code analysis tool to detect code security defects prior to production?	CUNA Mutual Group leverages third party code reviews to detect security defects beyond the peer code reviews.
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 SSAE16 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 leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	CUNA Mutual Group utilizes industry standard encryption methods to ensure confidentiality of sensitive information. A minimum encryption level has been established for both transmission of data and credentials and storage.
How is CUNA Mutual Group's data protected?	Information Security has implemented various controls within the organization. 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?	For our employees, CUNA Mutual Group utilizes multi-factor authorization for remote access to our internal networks.
Do you have documented information security baselines for your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	We maintain baseline hardening guides or group policies for our infrastructure components.
Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	Yes, we have a Security Incident and Event Monitoring solution, we do testing with our third party for penetration testing and we have a team who performs vulnerability testing on a regular basis. Live update features are utilized to ensure virus "signatures" remain current, or can be deployed real-time as signatures become available during a crisis.
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.) In addition, this plan is periodically tested.
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: · PCI Attestation of Compliance for Self-Assessment · SSAE 16 SOC 1 Type 2 – Pensions/Retirement Services · SSAE 16 SOC 2 Type 2 – Lending, CBSI and TruStage/Member CONNECT · Third-party Penetration Testing 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, utilizing a segmented (zoned) network. We have incorporated network-based intrusion detection prevention (IDP), data loss prevention (DLP), file integrity management (FIM), and content filtering.
Are passwords required to be changed?	We have robust password requirements, and CUNA Mutual employee user passwords are required to be changed at least every 90 days. The previous 8 passwords are remembered so they can't be used again. Passwords are never to be shared.
Does CUNA Mutual Group have physical controls?	Yes, we utilize multi-factor access control card readers, personalized access badges, visitor control points, CCTV and on premise security officers.
Are mechanisms in place to detect the presence of unauthorized network devices for a timely disconnect from the network?	Yes, CUNA Mutual Group has implemented security mechanisms to continuously monitor its network for unauthorized SSIDs.
Has an information security risk assessment been conducted in the last 12 months?	Our internal security governance framework includes several security policies and standards. Adherence to framework requirements is reviewed throughout the organization by multiple independent assessors including insurance examiners and multiple external audit firms.
Do you provide or make available a formal security awareness training program for on premise and/or cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?	CUNA Mutual Group employees affirm receipt of and compliance with our security policies and Code of Conduct through an Annual Disclosure process. Formal training is provided as are general awareness communications on various 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.
Do your data and virtual machine management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?	Yes, we utilize file integrity monitoring tools to ensure that virtual machine and all other file management controls remain intact.
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.

Question	Response
Business Continuity	
Does CUNA Mutual Group have a disaster recovery plan?	See the Business Resiliency Disclosure in the packet.
Has a Business Impact Analysis been performed?	See Business Resiliency Disclosure in the packet. Note: Business Impact Analyses for all business functions are regularly conducted. Proprietary information such as when the analyses are performed 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. CUNA Mutual Group is a separate entity that engages in joint marketing with credit unions.

5. **Does the GLBA prohibit financial institutions from sharing information such as Social Security numbers and date of birth with nonaffiliated third parties?**

   As long as credit unions notify members in their privacy notices that they share nonpublic personal information, credit unions can share this information. 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.

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. Note that 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 Document Samples*" on the left-hand side of the page; then go to "*Consumer Documents*" catalog).

8. **With the amendment to the Gramm-Leach Bliley Act 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.

   On October 20, 2014 the Consumer Financial Protection Bureau (CFPB) finalized a rule that allows financial institutions to post their annual privacy notices on-line instead of delivering them individually if they meet a series of conditions, including not sharing the customer's nonpublic personal information with nonaffiliated third parties. This recent GLBA amendment improves on the CFPB's rule, because it 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.

Both the GLBA amendment and the CFPB rule generally apply to those 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.

Merkle Inc.

Data Handling and Security Practices Summary

Introduction: Merkle is a Data-Driven, Technology-Enabled Performance Marketing Company. Started in 1988 Merkle has over 400 world class clients and 3400+ employees in 21 locations around the world. Our experience and superior reputation in the field of data security offer the high standards and confidence you expect, including:

- Safe and secure membership file encryption and convenient automated payment options
- SOC 1 audits performed annually to ensure compliance with industry standard security controls
- Data providers are required to strictly adhere to Merkle's Global Information Security Program, which is compliant with the ISO27001/2 security standards

Data Retention Limitations: When a credit union's membership file is received for billing or marketing services, the source data file is processed, verified, and then deleted from the network file server once it's processed. Files are then backed up daily with a 6 month retention period.

Business Extranet Access Policy: Access to Merkle's online services are limited to credit union employees and credit union data suppliers and is secured by user ID and password. The initial password must be changed immediately and thereafter the password must be changed every 90 days.

Data Transmission Security: To maintain the privacy of both the credit union's business data and the member's private data Merkle employs SFTP/Sterling/PGP/SSL encryption for our online business services that require data transmission.

Reliable Connectivity: Merkle provides daily support and file processing Monday through Friday from 8:00 a.m. to 5:30 p.m. CST.

Computer Viruses and Malicious Software: Merkle uses antivirus/ antispyware programs with central management and individual desktop firewall and intrusion prevention software.

Firewalls: Merkle deploys a multitude of interwoven, enterprise class security approaches. Our network is protected by a multi-layered firewall -deny by default rule sets. We also employ network intrusion prevention systems and data loss prevention system.

Data Backup and Recovery Procedures: Merkle always strives to prevent interruptions and uses commercially reasonable efforts to recover client hosted solutions in the event of a disaster. Periodic business impact analysis and annual corporate disaster recovery testing is completed to prepare for a disaster. Credit Union data is backed up daily with a 6 month retention period.

Employee Security: Merkle employees undergo background screening upon employment and each employee signs a confidentiality and nondisclosure agreement and participates in annual security awareness programs.

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 at Esurance

REVISED: May 12, 2016

FormNumber-MMYY

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: May 12, 2016

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.
- Annual reports are available at GoHealth

REVISED: May 12, 2016

LeadCloud 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 SSA# 16 reporting, compliance with Gram-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 and architecture in place to protect all personal information of their policyholders
            - All data consumed by LeadCloud is encrypted using https outside their firewalls. Data moving between services within the LeadCloud firewall is encrypted using TLS.
            - The LeadCloud solution is hosted in the Amazon AWS cloud. All AWS firewall technology is applicable and LeadCloud uses a multiple firewall layer architecture. LeadCloud uses an Internet Gateway (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html) that accepts internet traffic and forwards through a firewall to a set of load balancing servers in their private cloud which use Elastic Load Balancing (https://aws.amazon.com/elasticloadbalancing/). The load balancers route through another firewall to a set of web servers where the transactions are processed. Each type of server in their private cloud has its own subnet and firewall access controls. The Internet Gateway and their NAT are the only servers which have a public IP address.
        - Our partners ensure physical security measures are in place to control physical access to systems or outputs that contain personal data and privileged information.
            - See https://aws.amazon.com/security/ for more information on Amazon AWS Physical Security.
        - All data will be removed from operational data stores within 7 days of receipt. All back-up data will be destroyed in accordance with the data retention policy.
    - Data privacy
        - LeadCloud will only use the data received through this program to provide information needed for the insurance carrier to provide a real-time quote. All data received will be destroyed in accordance with the data retention policy.
- To learn more about LeadCloud, go to www.leadcloud.us.

Sutherland Global Services

Overview and Security Practices Summary

Introduction: Sutherland (SGS) is a process transformation company whose customer engagement transformation specialized services include customer experience expertise and contact center management. Headquartered in Rochester, N.Y., Sutherland employs thousands of professionals spanning 20 countries around the world. Our call center will be located in Virginia, with virtual agents and other centers across the United States. SGS agents will only take calls related to TruStage.

We are confident in the capabilities Sutherland provides to manage our consumer sales calls, while providing the best in consumer experience, scale and flexibility we need to meet expectations today and in the future.

Consumer Interactions: SGS will follow CUNA Mutual Group policies and procedures when interacting with consumers who contact the Sales Contact Center under Consumer Sales. All transactions will be managed using CUNA Mutual Group's Customer Relationship Management system.

Services Rendered: SGS will only operate within the United States for inbound call handling for the sale of life insurance and Accidental Death and Dismemberment insurance. All sales agents will be licensed in the United States.

Reliability: SGS will provide acceptable staffing levels to meet our sales plans, service level standards, and to adhere to CUNA Mutual Group standard hours of operations. Our current hours of operations are: M - F 7AM to 9PM CST, and Saturday 8AM to 4PM CST. CUNA Mutual Group may adjust hours of operations as business needs dictate.

Data Retention Limitations: SGS will not store CUNA Mutual Group consumer data. CUNA Mutual Group retains and maintains control of its consumer data in the same manner as it did previously.

Employee Security: In addition to licensing and continuing education to retain licenses, SGS employees undergo background screening prior to employment, and each employee signs a confidentiality and nondisclosure agreement and participates in annual security awareness programs.