Shastic

Due Diligence

727 Allston Way
Berkeley, CA 94710
408.600.0540

www.shastic.com

About the Company

Shastic was the first company to provide lending software solutions to financial institutions on Facebook in 2012, followed by the introduction of "Elle", Shastic's text-messaging platform. "Elle," is a software solution designed to help credit unions more easily communicate with their customers and loan applicants. Elle is a "plug and play" solution, facilitating high-touch, instantaneous, personalized engagement with customers through text messaging between banks and bank customers.

Since 2017, Elle has successfully been deployed at nearly 30 credit unions throughout the country, increasing the productivity of loan processing at these credit unions by upwards of 300%. Shastic has worked with over 100 different financial institutions across the country, and has established key partnerships with mobile banking providers such as Access Softek, which services over 400 financial institutions, and MeridianLink, which services over 800 U.S. financial institutions.

Shastic is a Delaware corporation, incorporated on April 22, 2009, in good standing with the state of Delaware. Shastic is backed by Berkeley Ventures, a high-tech business accelerator located in Berkley, California, which has backed dozens of early-stage startups.

Non-Mission Critical Application

We currently work with close to 50 credit unions in the U.S., and our clients have determined that we are a non-mission critical vendor. We do not connect to the institution's core or otherwise have access to any account or sensitive member or financial data of any kind.

Statement of Financial Condition

Attached to this package you will find a statement of financial condition for Shastic, Inc. This information should satisfy your vendor review process.

Security & Infrastructure

Shastic offers fully-hosted and maintenance-free solutions. Shastic's entire IT infrastructure is provided and managed by Amazon Web Services (AWS) at remote undisclosed locations. By leveraging one of the world's most secure and reliable IT infrastructure providers, we ensure that your data is securely stored and accessed.

The security features of our products have been reviewed and approved by many financial institutions. We enforce and support the following controls:

1. Secure access. Access points allow secure HTTP access (HTTPS) so that we can establish secure communication sessions with our services using TLS/SSL.
2. Built-in firewalls.
3. Encrypted data storage using the industry standard AES-256 encryption algorithm.
4. AWS cloud infrastructure has been designed and managed in alignment with regulations, standards and compliance best-practices.
5. Automatic remote backups nightly.
6. All IT resources are operated within an AWS Virtual Private Cloud (VPC).
7. Encrypted (TLS/SSL) connections for all interactions with our IT Infrastructure. We support the following SSL/TLS protocols: TLS 1.3, TLS 1.2, TLS 1.1, SSLv3, SSLv2.
8. All access to IT resources is guarded by Asymmetric key-pairs and multi-factor authentication.
9. AWS Identity and Access Management (IAM) roles and ACLs to segment and isolate like-functioning areas of the Infrastructure.
10. Separate development and production accounts to isolate the production system from development work.

The Shastic platform is hosted in Amazon Web Services data centers, which comply with ISO 27001, SOC1, SOC2 and SOC3 security management standards. Shastic receives updated SOC reports from our IT infrastructure provider AWS twice a year over a period of 6 months – Oct 1-Mar 31 and Apr 1-Sept 30.

In addition, Shastic implements SSL encryption for authentication and when transmitting data with end-users.

For more information regarding AWS's security, compliance and certifications, please visit:

http://aws.amazon.com/security
http://aws.amazon.com/compliance
https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf

Encrypted Text Messaging Communication

Shastic supports encryption via SSL (HTTPS) to protect communications between Elle and your end-users. The text messaging platform also supports the TLS cryptographic protocol.

Shastic strictly follows TCPA rules and regulation to ensure we are in compliance. Please see our *Text Messaging Guidelines* for more details.

Data Lifecycle

Shastic maintains the security and confidentiality of sensitive information and will use it only for the purpose of the scope of services. Shastic retains data encrypted at-rest for a minimum of 4 years as required by TCPA guidelines and for auditing purposes. Upon request Shastic can destroy any of the data stored related to your organization.

Shastic secures data in-transit and at-rest using the industry standards TLS, SSL, and military-grade AES-256 encryption.

Shastic leverages Amazon CloudWatch Logs to monitor and manage log files. In addition AWS CloudWatch automatically purges log files every 3 months.

Shastic uses AWS CodeBuild, a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. In addition, we leverage CodePipeline to automate the build, test, and deploy phases of our release process every time there is a code change. This enables us to rapidly and reliably deliver features and updates.

Text Messaging Guidelines

In 2015, FCC released a Ruling and Order concerning the Telephone Consumer Protection Act (TCPA) that immediately addressed text messaging and consumer protection. Here are the highlights:

- FCC reaffirmed text messages are subject to the same consumer protections under the TCPA as voice calls.
- Written consent is required before sending any marketing text message to a consumer mobile phone.
- "On demand" text messages sent in response to a consumer request are not subject to TCPA liability.
- Required to retain records of communication related to business made through text messaging applications.

As a response to these requirements, Shastic follows these best practices below:

- Ensure legal compliance with the TCPA and FCC rulings.
- Only send message to legally obtained opted-in numbers.
- Obtain prior written express consent from contacts before sending messages.
- Document and save program opt-ins and permissions

Opting-in
Thanks to the E-SIGN Act, prior written consent may include electronic or digital forms of signature. These include agreements obtained for text message opt-in via email, website form, text message, dial pad or voice recording.

Opting-out
According to the TCPA, your contacts should have the ability to opt-out at any time.

How Shastic Manages Opt-outs
When a contact sends STOP, STOPALL, UNSUBSCRIBE, CANCEL, END or QUIT to one of your numbers, Shastic will prevent them from receiving any additional messages until that contact responds START. We then place that contact in the default 'Stopped' group. The contact is removed from all other groups and specially marked so that any outbound message attempts are blocked.

Sending Timeframe
The TCPA stipulates that text messages may only be sent between 8 a.m. and 9 p.m. in the time zone your recipient is in. If your service sends messages to contacts in different timezones, contact us about the various options we provide.

Record Keeping
Shastic keeps your data secured and encrypted at rest for four years. To protect your organization from future disputes, it's advisable to maintain each contact's consent for at least four years from that date in which it was given, which is the federal statute of limitations for bringing an action

under the TCPA.

For more information, please reference the FCC rulings on TCPA.

Further questions

Please refer any further questions you may have to us via support support@shastic.com. Thank you for the opportunity to work with you and your financial institution.

Sincerely,

The Shastic Team