MobileGuard, Inc.

Briefing on our solutions

REVISION Q1 2016
(PUBLIC VERSION)

What do we do?

MobileGuard provides mobile compliance solutions for organizations internationally around text messaging, mobile call recording and secure messaging. We do so with three product lines:

1. **MessageGuard**^{TM} – an app-powered solution for Android and Blackberry that is carrier neutral. The app is installed from the Google Play Store, via direct URL or mobile device management solution (MDM), and captures SMS/MMS messages from the native messaging application, for archiving and supervision.
2. **NetGuard**^{TM} – a pioneering solution based on carrier integration, allowing for native SMS/MMS message archiving from any device capable of sending text messages on a carrier's network. This includes Android, Blackberry, iOS and Windows mobile devices as well as feature and flip phones.
3. **SecureChat**^{TM} – an installed application that provides secure, encrypted messaging, with attachment support, for any organization that requires an alternative to native text messaging communications for regulatory or governance purposes. What markets do we serve?

- Corporate enterprise, including the Fortune 1000
- Financial Services
- Government at the Local, State, Regional and Federal level
- Healthcare
- Legal
- Transportation

What do we do with the data we archive?

Our solution includes an Administrative console for accessing the archived messages; including SMS/MMS, mobile call audio and data archived using SecureChat^{TM}. This data can be searched, downloaded and reported on. In addition, MobileGuard will support integration with your internal archiving system and send this data to that location.

Who do we integrate with?

Our integration efforts work on three tiers:

1. Carriers/Operators
2. Mobile Device Management solutions (MDMs)
3. Enterprise storage providers

Customers benefit from our integrations with MDMs and enterprise storage providers. See below:

MDM

A customer may use an MDM to distribute and manage our app solutions (MessageGuard and SecureChat) to their user base. This also addresses how app updates are delivered. For customers not using a MDM solution, the primary method of app update is via the mobile app stores.

Customers may also use an MDM to distribute and manage their mobile device policies. This includes disabling iMessaging on iOS to insure only native SMS/MMS messaging is available as the Messaging application on iOS devices.

Enterprise Storage Providers

These are often used for email and other related message archiving storage and management. Some customers also use solutions which are broader beyond messaging and satisfy all of their eDiscovery needs (files, multimedia, imaging, et al).

MobileGuard can deliver the data we archive to those systems to add SMS/MMS, mobile call audio and secure messaging into those dashboards as a convenience to our customers.

What role does the carrier play with our product lines?

Carrier Roles	**MessageGuard**	**NetGuard**	**SecureChat**
SMS/MMS Routing	N/A	X*	N/A
NOTES: * Carrier may offer access to existing API for MobileGuard to access and acquire data. Carrier may also sequester data to be archived and store on messaging server for MobileGuard to pick up.			

Are our solutions visible to the carrier, and also, to the users of each solution?

MessageGuard – is an app installation on each licensed mobile device. At minimum, it is visible to a MDM solution managing those devices, and most likely to the end users of the mobile device. The end users continue to use their native texting capabilities while the app runs silently in the background of the device. It is a carrier neutral solution not requiring interaction from a carrier/operator.

NetGuard – is invisible to an end user as a presence on each mobile device. However, to activate NetGuard on any mobile device requires a provisioning SMS message to each mobile device, and user opt-in to activate on the carrier network. The devices can be managed by an MDM, but no application installation or maintenance is required on the mobile device beyond the provisioning step.

NetGuard is visible to the carrier/operator at their network level of operations due to integration.

SecureChat – this is an app installation solution that causes the mobile device user to leverage SecureChat as their primary messaging solution. A customer must disable native messaging via the carrier on mobile devices using SecureChat. SecureChat is a carrier neutral solution not requiring interaction from a carrier/operator.

How are iOS devices supported in our solutions?

MobileGuard is an Apple partner and is able to support SMS/MMS message archiving on iOS devices being operated on an affiliated carrier network. Customer predominantly disable iMessaging (leaving only SMS/MMS messaging active) using a MDM solution in conjunction with Apple's DEP program[i].

How is data transfer secured between end users, carriers and our solution?

All data transactions are handled in accordance with federal law. MobileGuard follows all federal, State and local requirements for data transfers. Additionally, MobileGuard has built in various safeguards to ensure the safety of confidential data, such as our on premise model.

Additional security measures are accommodated in SecureChat to insure encrypted messaging to satisfy customer and/or regulatory requirements.

How long do we store the archived data?

MobileGuard retains the data for as long as stated industry or government retention policies. If departing as a MobileGuard customer, all data will be transferred to the organization. We may use varying data center environments to accommodate additional regulatory requirements.

Can a business run a trial or pilot with our solutions?

Trials	**MessageGuard**	**NetGuard**	**SecureChat**	**VoiceGuard**
	30 day free trial on 5 devices	Free 30 day trial on up to 5 devices*	30 day free trial on 5 devices	Can test existing line on carrier for 30 days (one line)
NOTES: * Can opt for paid pilot for larger universe of devices for up to 6 months as proof of concept.				

[i] https://www.apple.com/business/dep/