

The Importance of Mobile Messaging Compliance

An Osterman Research Executive Brief

Published January 2010

SPONSORED BY TEXTGUARD, INC.

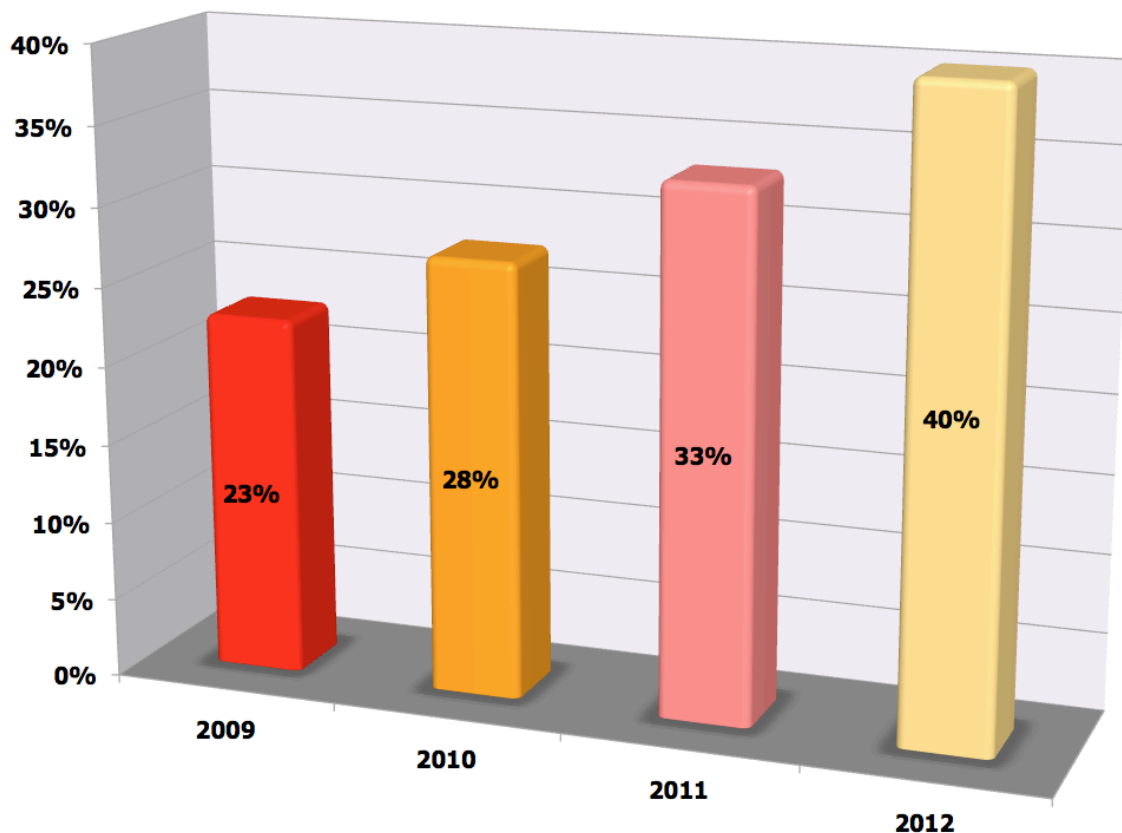


The Growing Importance of Mobile Messaging

Mobility in its greater context – namely, enabling employees to work from any location – is becoming more common as a means of increasing organizational flexibility, reducing operating expenses, reducing taxes and improving customer service. Mobile messaging is a key component of this trend by enabling properly equipped workers to send and receive email, access the Web and Web 2.0 applications, use corporate applications and communicate in a variety of ways regardless of where they work.

As shown in the following figure, growth in the proportion of the North American workforce that uses company-supplied mobile devices – not to mention those that use their own mobile devices for work purposes – is on the increase.

**Workforce That Uses Company-Supplied
and Company-Funded Mobile Devices
2009-2012**



It is important to note, as well, that smartphones represent the bulk of mobile devices used in the workplace today, and that smartphones are the part of the mobile device market that is continuing to grow at a healthy pace despite the current recession. Further, roughly two-thirds of smartphones today use 3G networks, enabling mobile

workers to more closely replicate their office experience for email, application and Web access.

What all this means is that mobile messaging will continue to grow at a strong pace throughout the next several years, driven primarily by the need to mobilize the workforce in an effort to reduce overall corporate costs, speed decision making and improve employee efficiency. While mobile capabilities will displace some traditional computing and communications, the primary effective will be additive as organizations layer mobile messaging capabilities in with the rest of the communications and computing infrastructure they already have in place.

The Growing Liability of Mobile Messaging

Although mobile messaging carries with it the promise of significantly enhanced employee productivity, faster decision making and greater overall efficiency for organizations of all sizes, it also carries with it a number of quite serious risks. Among these risks are:

- **Loss of sensitive or confidential data**

In a survey of mid-sized and large organizations conducted by Osterman Research in 2009, the most serious problem faced by organizations in the context of their mobile messaging use is the loss of corporate data in the event a device is physically lost. That survey found that 39% of decision makers consider the risk of data loss in the event of a lost device to be a serious or very serious problem.

- **An inability to archive mobile content**

Another survey conducted by Osterman Research during 2009 found that 20% of corporate data in mid-sized and large organizations is contained on mobile devices of various types. However, few organizations have a way of archiving this content in order to comply with their legal or statutory obligations, or with their corporate policies.

- **An inability to monitor communications sent via mobile devices**

Organizations must be able to monitor communications to detect policy or legal obligations. For example, financial institutions, energy-trading companies and others must be able to prevent or limit communications between certain departments or functions within their organizations. However, most organizations today cannot do so for their mobile users, meaning they are exposing themselves to a variety of risks, including legal sanctions and enormous financial losses.

- **Violation of compliance obligations**

There are a growing number of obligations with which virtually every organization must comply. These obligations, which are focused primarily on the archiving, encryption and monitoring of certain types of communications, include the following:

- Rules established by the **SEC, FINRA, FSA** and other regulatory bodies are focused on financial services organizations' obligations to monitor and archive

communications between broker-dealers and their customers. These include inter-office communications and various types of advertisements, testimonials and other content.

- The **Federal Rules of Civil Procedure** obligate organizations to manage their data in such a way that their data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.
- The **Gramm-Leach-Bliley Act** requires financial institutions to protect sensitive information about individuals, including their names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.
- The **Federal Information Security Management Act of 2002** is a far-reaching law that requires every agency within the United States Federal government to develop and manage an information security plan for every information asset it owns.
- The **Health Insurance Portability and Accountability Act (HIPAA)** requires healthcare and other organizations to protect sensitive health records of patients and others. However, the “new” HIPAA that takes effect during the first quarter of 2010 greatly expands the impact of the law. For example, while HIPAA previously applied mostly to physicians, medical practices, hospitals and the like, now the business associates of these entities will be required to comply with HIPAA’s rules about the security and privacy of protected health information (PHI). That means that accountants, benefits providers, attorneys and others that are given access to PHI will now be fully obligated to comply with HIPAA.
- The **Payment Card Industry Data Security Standard** is a set of requirements for protecting the security of consumers’ and others’ payment account information. It includes requirements for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.
- The **Sarbanes-Oxley Act of 2002** obligates all public companies and their auditors to retain relevant records like audit workpapers, memoranda, correspondence and electronic records – including email -- for a period of seven years.
- The **Federal Information Security Management Act of 2002 (FISMA)** requires the transparency of transactions and the types of information that must be captured when clients place trades. MiFID specifically requires instant messaging compliance by retaining conversations that reference trades.
- **Federal Energy Regulatory Commission** Order No. 717 imposes various rules on regulated and vertically integrated utilities so that transmission providers do not give preferential treatment to their affiliated customers. The purpose of

this order is to create an ethical wall between the marketing and transmission functions of vertically integrated companies that distribute electricity and natural gas between states.

In short, organizations face a variety of risks from their inability to properly manage, secure and archive the use of mobile devices in their organizations.

What Should You Do for Mobile Messaging Compliance?

Clearly, organizations of all sizes must use mobile capabilities. The efficiencies, productivity and competitive advantage that mobility affords can provide an organization with enormous benefits in both the short- and long-term. However, organizations must also mitigate the risks associated with mobile device use, including the potential loss of sensitive and confidential data stored on mobile devices, the violations of various statutes that can occur if communications are sent improperly, and violations of various legal obligations and statutes if the content on mobile devices is not archived properly.

The answer, then, is to deploy a capability that will permit mobile devices to be used as freely as possible by as many people in an organization as necessary, while at the same time allowing IT to manage these devices and the content that users send and receive with them.

It is also important, if at all possible, to use a mobile compliance solution for mobile users that will integrate well with an existing archiving solution designed to archive email and other electronic content. There are two important advantages to doing so:

1. Mobile content will be preserved in the primary archiving platform maintained by an organization. Osterman Research surveys have shown repeatedly that most organizations would prefer a single archive for all of their electronic content instead of a growing series of silos for different types of content.
2. By integrating mobile content with the primary archive, administrators and others do not have to learn a new interface, allowing them to add mobile content to the archive without the burden and learning curve often associated with adding a new capability to the mix of what they must already manage. This is particularly important for non-technical types, such as legal counsel or senior business managers, that often access an archive themselves to search for content in support of regulatory review, e-discovery or other purposes.

A Proven Mobile Compliance Solution

TextGuard provides a complete mobile device compliance solution and ensures messaging compliance mandates with all regulatory bodies. The solution provides logging, archiving, monitoring, supervision and alerting of a company's mobile devices.

The Importance of Mobile Management and Compliance

Presently compatible with Windows®, Blackberry® and Android®, these features are available for text messages, (SMS), Blackberry PIN messages, as well as BlackBerry® Messenger.

TextGuard's mobile electronic communication compliance platform is available as a SaaS or on-premise solution and can be implemented within days as a supplement or complement to an organization's existing archiving and compliance solution. TextGuard works independently of the BlackBerry Enterprise Server (BES), but can be easily integrated with its policies.

TextGuard prides itself on its reputation of professional customer support, and it wants to ensure that all of its customers have a "beyond satisfactory" experience. The company is dedicated to ensuring that all of its mobile messaging compliance solutions are properly integrated with its customers' system and that any technical issues are resolved quickly. The company can manage everything from initial implementation to records migration and anything that comes up in between. TextGuard is committed to making its customers' transition to its messaging compliance platform as streamlined as possible.

TextGuard's enterprise compliance solutions support gives customers variable levels of service depending on their budget and desire for technical assistance. Companies lacking a comprehensive IT department can also make use of TextGuard's professional services if its customers need customization of our existing application.

For more information, TextGuard can be contacted at:

**131 N. Michigan Avenue
Kenilworth, NJ 07033
+1 646 924 3420
helpme@textguard.com
www.textguard.com**

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.