



TextGuardTM
MOBILE DEVICE SECURITY

Information Security Regulations in Critical Work Areas

Compliance with SMS (Short Messaging Service)

A White Paper

May 18, 2009

Information Security Regulations in Critical Work Areas

The crises witnessed in major financial institutions the world over in the recent past have forced such financial institutions to scrutinize the informational security environment in their organizations. There is a very real fear that critical information communicated out of a secured work area may generate a disastrous financial landslide. For this reason, regulatory agencies have set up stringent informational security regimens suitable to the industries and processes they watch over. It is now mandatory for institutions in the securities, banking, insurance, mortgage, health and similar economically-critical sectors to implement the security regimens prescribed by the competent regulatory agency.

Ensuring compliance with the prescribed security regimen is extremely difficult in general and specially in the case of Smartphones, PDA's and other handheld communication devices. The business that cannot ensure compliance with the prescribed security regimen may face demotion in its quality-of-service (QoS) rating. The same applies to its financial credit rating. This will adversely impact the credibility of the business in the eyes of its clients, customers, suppliers and associates. If the business cannot maintain customer confidence regarding its internal information security then there is a very real danger that it may lose its reputation overnight and that can be disastrous to the business! This must be avoided at all costs!

Almost every business with informational security concerns has implemented a monitoring system to ensure compliance with the norms prescribed by the regulatory authority.

Electronic communication media place a special burden on security-conscious institutions. Office computer networks are connected to the Internet as a rule rather than as an exception. Emails, file transfers and instant messaging services provide convenient means of communicating information out of the secured work area. PDAs and mobile phones with advanced features are functionally equivalent to computers when it comes to transferring information out of the secured work area. Such wireless communication devices are harder to supervise and control compared to wired computer networks. Regulatory agencies have noted this weakness and have addressed it very specifically.

The problem is compounded by the fact that mobile communication devices (read 'Smartphone') are becoming ubiquitous in general and more specifically among the executives who are in high-risk security zones. One option is to ban the use of Smartphones in the high-risk security zones. This may require a physical check (frisking), which is both not very practical and hard to implement. The intelligent option is to install and implement a Smartphone monitoring application on company devices that need regulatory compliance.

The objective of this white paper is to elaborate on the modalities of implementing a Smartphone monitoring solution on Mobile Devices, (Smartphones) which are used for company purposes.. We shall focus on the use of the TextGuard Smartphone Security Solution to guarantee compliance with regulatory requirements.

Monitoring Smartphone's To Meet Regulatory Requirements

Introduction

Watchdog regulatory bodies operating in different sectors have set up industry-specific guidelines and compliance checklists to prevent sensitive information from leaving designated security zones. They are concerned that this sensitive information may be used by perpetrators to extract an unfair financial advantage. Regulatory compliance is rapidly becoming mandatory in a growing number of business sectors.

Smartphone's are advanced mobile devices that can be used to communicate sensitive information in a number of ways. Their mobility makes it difficult to implement simple regimens to monitor them. They are small enough to be carried around the premises undetected. The multiplicity of ways, the mobility and the lack of size combine to make Smartphones a security manager's worst nightmare.

Businesses must take steps to protect themselves from information leakage for their own sake. With the added burden of regulatory compliance, businesses cannot afford to ignore this vital issue anymore. However, the IT departments of most businesses are not technically equipped to secure the sensitive information, especially when dealing with Smartphones. It is imperative that businesses that require regulatory compliance upgrade their information security systems on a priority basis. They MUST choose a system that is durable – it is of little use to install and implement a Smartphone's monitoring system that is dated and limited in technological foresightedness.

Security Regulations and Communications

Recognizing the fact that "knowledge is power", and that information is the precursor of knowledge, authorities concerned with the welfare of the investing public have developed and defined regulatory procedures and checklists to prevent the misuse of privileged information.

For example, FINRA (Financial Industry Regulatory Authority) regulates the SEC-traders. They have issued a Customer Information Protection notification which says:

"Protection of financial and personal customer information is a key responsibility and obligation of FINRA member firms. Under the SEC's Regulation S-P, firms are required to have policies and procedures addressing the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information and against unauthorized access to or use of customer records or information."

Similar regulations have been issued by other regulatory agencies such as HIPAA (Health Insurance Portability & Accountability Act - for the healthcare sector), SOX (Sarbanes-Oxley Act - for public companies), and the FTC (Federal Trade Commission - the Fair and Accurate Credit Transactions Act, 2003, and the Red Flags Rule applicable across the board to all businesses and financial institutions).

Compliance with the regulatory requirements of these supervisory authorities is mandatory for institutions and businesses operating in the ambit of the respective regulatory agency. The IT departments of such institutions must enforce suitable security regimens to ensure regulatory compliance.

As a first step in this direction, an organization must define the sensitivity of information – high, medium and low – according to its prospective adverse impact on the organization itself and on the people who have a vested interest in the organization. The second step is to identify the persons who have a valid reason to access and use the information; in other words, a person must be authorized to access and use the sensitive information. The third step is to define the areas where such information is generated and used; in other words, a 'security cage' must be defined for each type of sensitive information.

The regulatory bodies require the organization to ensure that highly sensitive information remains restricted in access to authorized persons exclusively. As a corollary, sensitive information must remain within its security cage. Smartphones, unfortunately, present a very real and potent danger in maintaining informational security in the workplace. Hence, extreme caution must be exercised to make Smartphones acceptable in the workplace whilst maintaining compliance with industry-standard regulatory norms. An institution's information resource may be compromised in a number of ways. These are:

External attacks: An external agency attempts to access the institution's sensitive information using trojans and similar malware, by using sophisticated radio communication equipment, or by hacking. A Wi-Fi access point (AP) in the institution's vicinity is a potential security risk.

Internal events: The main types of internal events that may compromise sensitive information are:

- *unauthorized interaction between employees;*
- *deliberate attempts to access sensitive information;*
- *deliberate attempts to convey sensitive information to unauthorized persons;*
- *unintentional transmission of sensitive information to unauthorized persons.*

Applying Security Regimens In A Smartphone Environment

Smartphones pose a great danger to the informational security environment because:

- *they are mobile;*
- *they are physically small and so, hard to detect;*
- *they communicate over multiple paths;*
- *they communicate using multiple protocols;*
- *they have a multiplicity of advanced functions that may provide unknown communication pathways;*
- *they are personal devices that are also used for business communications;*
- *they are business devices that are also used for personal communications;*
- *they are gaining popularity as the communication device of choice amongst executives;*
- *they are gaining popularity as the personal decision support device of choice amongst executives;*
- *they are prone to malware attacks;*
- *they are (most often) connected to the business' information network.*

The BlackBerry is rightly considered the epitome of Smartphones. However, as a result of patent infringement, the US District Court for the Eastern District of Virginia issued an order effectively shutting down BlackBerry services and operation in the US. A stay on the injunction allowed BlackBerry to continue its US operations.

In a surprise move, first the US Department of Justice and then a few months later, the US Department of Defense filed special briefs with the Court requesting it to vacate the injunction against BlackBerry operations. The reason cited by the DoJ was the large number of BlackBerry users in the US Federal Government. The reason cited by the DoD was even more spectacular. It stated that the BlackBerry was crucial for national security.

The "brute force" method to curb the problem of informational leaks due to Smartphones is to ban their presence within the security cage. Small firms may actually employ such a method where the number of Smartphones is low or zero. Such a method is impracticable in medium and large sized institutions where almost every executive carries a Smartphone and uses it as part of his personal decision support system. In such cases the institutions rely on special Smartphone monitoring software systems to maintain regulatory compliance.

At a minimum the Smartphone monitoring solution must be able to monitor and report security regimen violations with respect to email correspondence, SMS, (Text Messaging), IM, and PIN (this is a BlackBerry-specific communication facility). Desirable features in such monitoring systems include a protocol management system to set user authorities, access levels, define authorized groups, and sundries like restricting or allowing access based on time of day and day of week.

Using such a sophisticated Smartphone monitoring solution maintaining regulatory compliance is the intelligent solution to the problem of applying mandatory security regimens in a pragmatic way.

Applying Security Controls at The Device Level

The common objective of the various informational security regulatory systems vis-à-vis Smartphones is to control the information traffic through the Smartphone device. Smartphones are called that because they have many sophisticated features and facilities to manage and control the information flow originating from and terminating at the device. So if on the one hand Smartphones are a security and compliance challenge to information security managers entrusted with enforcing regulatory compliance in the workplace, then on the other hand they are extremely facility-rich in applying security regimens on individual devices.

A Smartphone can be programmed to implement a security regimen by setting the various options that are built into the device's operating system. These settings can be programmed by the user via the device's keyboard. Alternatively, and more importantly, the settings can be programmed wirelessly from a remote location. This latter method is referred to as "Over-The-Air" or OTA programming.

Similarly, software programs can be "pushed" OTA to the device and installed directly. Using this feature, a company's IT department can remotely install programs on Smartphones that are specially developed to enhance the device's native security features. The client program (the program that is installed on the Smartphone) becomes a cooperating component of the enterprise-wide information regulation compliance system. This is an invaluable feature indeed.

Of course the enterprise-wide information monitoring system (and its client component) must be tamper-proof, reliable, and well-designed in itself to provide meaningful information protection so that the business can meet security regulations. Besides this, the monitoring software system must be sufficiently avant-garde to cater to the technological and regulatory developments in the foreseeable future. The development of such software systems is an ongoing process by necessity. So the software development firm must be ready, willing and able to produce upgrades as these become necessary due to developments in security regulations and Smartphone technology.

Securing the Smartphone Device

A Smartphone poses a dual threat to an organization's information security environment in two key ways. Firstly a user can communicate with unauthorized persons and secondly, the user can access (not amounting to communicating) sensitive information in an unauthorized manner. Both these activities can jeopardize the company's regulation compliancy status.

IT departments, information security managers and regulation compliance managers must ensure that any Smartphone monitoring system they acquire and implement possesses Behavior Blocking and Information Protection and Control features. The security feature that prevents unauthorized communication is termed 'Behavior Blocking'. The security feature that prevents unauthorized access to sensitive information is termed 'Information Protection and Control'. An executive can use a Smartphone to access sensitive information residing on the firm's computer network. This is possible by using the Smartphone's Bluetooth capability or wireless network access capability.

Behavior blocking is most often implemented using white lists (a list of authorized contacts) and black lists (a list of unauthorized contacts). These lists must be updated regularly for them to be effective in ensuring security regimens in compliance with regulatory requirements.

The first step in securing a Smartphone device is to "register" it as part of the organization's information security environment. This is accomplished by a Smartphone management system running on the organization's computer network. The Smartphone management system may be supplied by the Smartphone vendor as part of the package, or it may be a separately procured package.

Supervising the Information Flow for Regulatory Compliance

Messages routed through a Smartphone must be reviewed by a competent executive to ensure that the security regulations have been adhered to. Hence a copy of every message must be stored someplace pending review.

The security executive checks whether the message was sent to an authorized recipient or not. He must also check whether the message contained unauthorized information or not. The messages must be logged and stored away for future reference in a properly organized and maintained archive.

The security executive reports cases of informational security regulatory violations to a competent authority within the organization. That competent authority then decides on a course of remedial action to be taken in accordance with the regulatory procedures. This is part and parcel of regulatory compliance. The person responsible for the regulatory violation may or may not be informed of his role in the violation depending on the organization's defined course of action and, of course, the regulatory requirement. Action against the offending person, again, depends on the organization's own regulations and the mandated regulatory requirement.

Messages may be transferred between executives of the organization (internal messaging) or between a company executive and an outsider (external messaging).

Supervising Internal and External Messaging

Supervision of internal messaging is necessary in those organizations implementing security cages. This is to prevent "insider" information from being used in an unfair manner. Another reason is to prevent undesirable exertion of influence by one executive to another. This virtual segregation of communicants is referred to as a "Chinese wall" by information security professionals.

When messages are sent to or received from an outsider, then the risk of a regulatory infringement increases. The security executive has to be extra vigilant when reviewing such messages compared to the vigilance required to review internal messaging. Additionally, some security regulations require the firm to keep a copy of messages sent to the firm's clients for a period stipulated by the regulatory authority.

If the firm uses a Smartphone monitoring solution then the platform should be able to provide all the facilities required to supervise the messaging via the Smartphone registered as part of the firm's security environment. The facilities must be convenient to understand and use. Reportage should be flexible and useful rather than voluminous. The system must be able to archive messages efficiently. If there is a regulatory requirement to store a class of message for xx days, then the system must have a facility to automatically store the specified message class for xx days, and archive the messages that have passed the stipulated xx days. The system must provide a proper log of all messaging activity. The system must also have a search facility to help a reviewer search for messages by content or message type or recipient or sender or any other suitable parameter.

In short, the software system must have features to assist in the review process associated with ensuring regulatory compliance.

Message Review Modes

Messages must be reviewed by a security executive to check for regulatory violations. Violations should be proceeded against according to established norms, both those of the organization and those of the regulatory authority. Every message transferred to and from a registered Smartphone must be copied to the security executive for review.

Depending on the volume of message traffic the security executive may review each and every message that is copied to him (or her) for review. This is done if the message traffic is limited and well within the reviewer's capacity. If the information is extremely sensitive (national security, for example) then each and every message is reviewed, no matter how heavy the traffic.

In most cases, however, a stringent scrutiny of each and every message is not called for. If practical statistics shows that an organization's executives mostly comply with the security norms then a fair sampling of messages, not all, are sent for review. Generally this fair sampling is selected in the following:

Lexicon selection:

Messages are processed by a computer program which checks the contents of all the messages for certain trigger words and phrases. Only those messages that contain the trigger words are reviewed by the security executive. These trigger words are contained in a compiled lexicon or word-list, maintained and updated by the organization's information security department.

Random selection:

The informational security department sets a quantum (e.g. 100 messages a day) or a percentage (e.g. 20% of the daily message traffic) as a limit for messages selected to be reviewed. A computer program then selects the stated number of messages on a random basis and sends them to the security executive for review.

The selection can be for incoming messages, outgoing messages, internal messages, external messages, department-wide messages, or any combination it sees fit. If the regulatory requirements require a particular selection criterion then that criterion is applied in the message selection process.

Message Storage, Management and Retrieval

Informational security regulations may, and usually do, specify that an organization keep a copy of messages for future reference. This is sometimes referred to as "cold storage" by information security professionals. The regulations may specify the types of messages to be kept, and the duration for each type. This is part of regulatory compliance. Hence an organization must implement a suitable message storage and retrieval system to ensure compliance. This system is referred to as an archival system. An archival system must be well-designed to facilitate message storage management and message retrieval.

Messages which pass the regulatory "cold storage" period can be trashed (deleted completely) or they may be vaulted, a storage system where all messages are highly compressed to save storage space, and rarely accessed. The idea is that messages once placed in the vault will never be required; still, they are there just to be on the safe side. After a sufficiently long time (e.g. twenty years) the messages are permanently deleted from the vault.

The message archival system must be capable of archiving all types of text messages that can be generated or received by a Smartphone. SMS is the general message format. BlackBerry Smartphone can communicate directly with other BlackBerry Smartphone using a PIN-based protocol. Other Smartphone are getting ready to follow suit in implementing this BlackBerry-PIN compatible messaging system or a variation thereof. The organization's message archival system must be capable of storing the BlackBerry-PIN messages and its variants when they appear in the Smartphone.

It is always a good idea for an organization to acquire software that works in cooperation with existing software. That way the organization doesn't have to duplicate its efforts in performing data entry, searching for records, record modification, or generating reports. But this is not an over-riding technical feature and can be played down in the acquisition of information monitoring solutions.

Organization's intending to implement software solutions to assist in maintaining regulatory compliance need to heed one piece of advice offered here: Don't wait too long to implement the security software solution! The communication field is wide open and expanding exponentially. Too often the security executives are taken in by trade announcements of impending releases - software or hardware - and wait for the release. Meantime the organization's sensitive information is left vulnerable and the organization open to scrutiny by regulatory authorities.

Technical blogs and sites are good sources of information relating to informational security in high-risk, high-security arenas. But be warned that there are some unreliable sites that thrive alongside the reliable sites.

The TextGuard Security & Compliance Solution

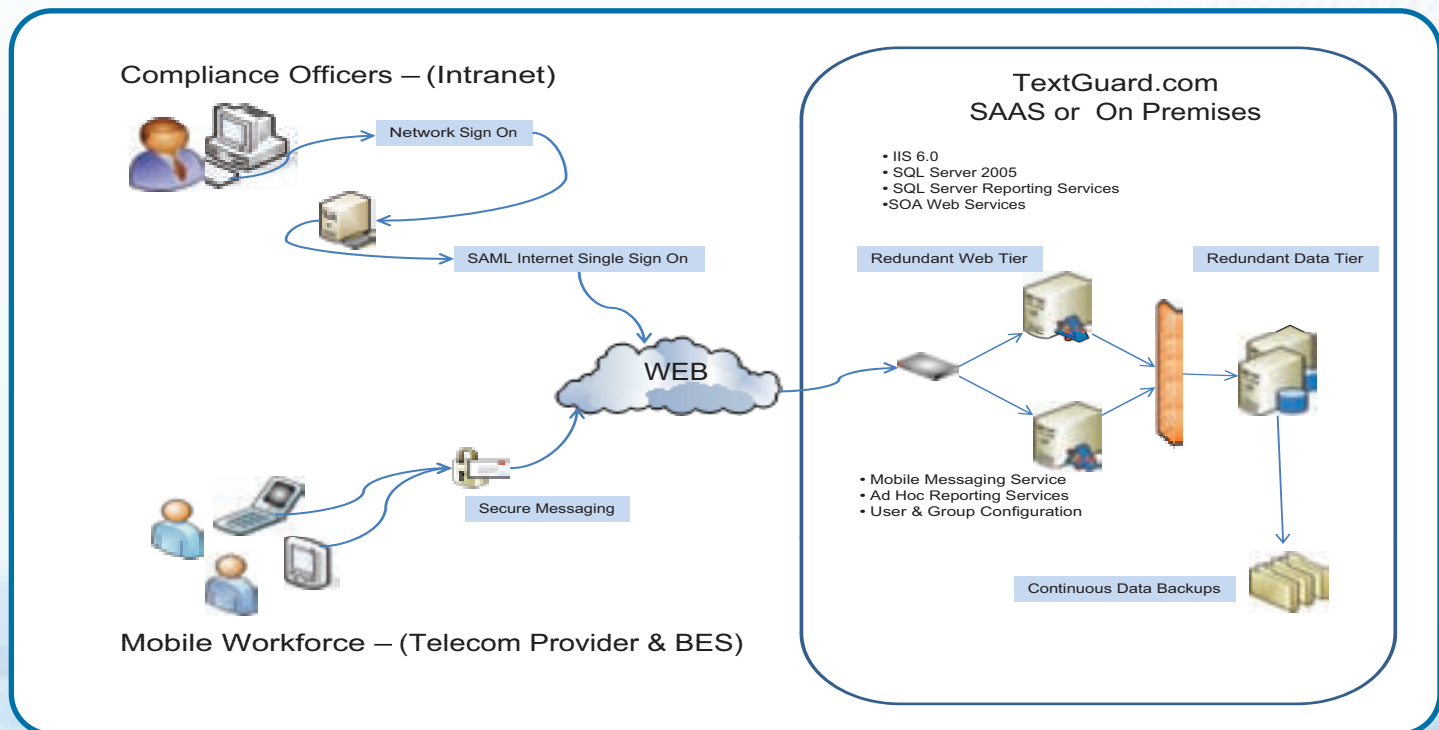
Preamble

TextGuard is not a "Topsy" software offering that "just grew" over a mocha, nor is it a product of chance that resulted from a net entrepreneur bumping into a barely-bearded youth flogging his latest brainchild.

At first glance, that statement might appear out of place in a white paper. But the fact is that this statement is more important than all the technical specs that follow. TextGuard was conceived with due diligence: technical analysis, market analysis, and feasibility analysis. The TextGuard product was designed in its totality with equal emphasis on technical excellence and market sustainability. Creating a technical gem is one thing, making sure that it stands its ground in the volatile IT marketplace is another thing. If a product is not sustainable then satisfactory client support is not maintainable either. And another "one-hit" wonder bites the dust!

TextGuard was designed by a group of technical and entrepreneurial stalwarts to be the best available Information Security Solution for Mobile Communication Devices. Every aspect of the TextGuard product has been given careful consideration to ensure its living up to its designed level of excellence. TextGuard has been designed to become a technical and entrepreneurial success and is creating new benchmarks in the informational security arena.

TextGuard is based on a future-ready design. Special features (many that have a patent-pending status) are being researched, designed and developed on a continuous basis. These features will enable TextGuard to operate in the ever-changing technological scenario for the years to come.



Specific Technicalities

- TextGuard is a binary product - it has two components: a server component, and a client component. The client component is installed on the individual smartphones, whereas the server program is either a hosted solution, (SAAS) or can be installed on the corporate computer network.
- The TextGuard server component applies an overall enterprise-wide information security regimen to all the smartphones in the organization.
- The TextGuard client component applies control to the smartphone device itself; this is also known as end-point security control.
- Security managers can manage the enterprise-wide information security regimen conveniently. An intuitive and well-designed user-interface allows the corporate information security manager to set and reset security rules for individual smartphones and for all devices.
- TextGuard is designed to work on ANY cellular mobile carrier.
- TextGuard operates under various device operating systems.
- TextGuard provides Layer A level of regulation-compliance for smartphones used in industries, businesses and organizations operating in a sensitive information environment.
- TextGuard monitors and logs all communications in and out of the smartphone. It selectively blocks incoming and outgoing calls.
- TextGuard selectively blocks access to web sites on select operating systems.
- TextGuard filters text messages (SMS and email) for obscene and prohibited content on select operating systems.
- TextGuard is rich in message archival management features.
- TextGuard is the only mobile security product that maintains its logs and archives on a secured server. The archives are accessible by an authorized user from anywhere in the world via the Internet.
- TextGuard facilitates legal discovery of information and data contained in text messages sent and received on registered smartphones.
- TextGuard maintains and manages a secured message archive. The contents of the archive can be used as trusted evidence in the judicial process.
- TextGuard archived messages are evidentiary, both unwriteable and unerasable.
- TextGuard lets administrators monitor an employee's communications. All messages can be archived. This prevents loss of corporate data when a smartphone is lost or stolen.
- TextGuard lets administrators lock a smartphone remotely. This is specifically useful in preventing unauthorized access to sensitive corporate data when a smartphone is lost or stolen.
- TextGuard operates over standard and non-standard data communication channels. For example, TextGuard monitors PIN-based messages between BlackBerry phones.
- TextGuard has all the features that an information security manager requires to establish a mandatory security regimen within the organization.
- TextGuard is useful in electronic communication compliance regulated industries like securities, banking, pharmaceutical, healthcare, accounting and hedge funds. In fact, any Fortune 1000 company or small business will also benefit from the TextGuard Solution given its advanced functionality and low price point.
- TextGuard recognizes the advanced features available in smartphones today and those that will become available in the future. It makes full use of these features to give the user complete control over the security of sensitive information passing through the smartphone.
- TextGuard is the most comprehensive sensitive information security solution available at a very affordable price point.

Chinese Walls - TextGuard facilitates maintenance of white lists and black lists to control communication between the smartphone user and respondents. The control extends to all types of devices and communication modes: SMS/HTTP/PIN.

Content filtering - TextGuard facilitates maintenance of lists of trigger words and phrases to help in filtering suspicious messages. The admin can include trigger words that recognize sexually aggressive messages aimed at women, sexually abusive messages aimed at children, coercive and threatening messages and racially offensive messages.

PIN-recognition - TextGuard recognizes the PIN-feature of smartphones. It uses this feature to prevent message delivery to the wrong recipient.

Advanced archive management:

- *TextGuard is the perfect solution to archive management issues.*
- *The TextGuard archive manager is designed to facilitate e-discovery requirements and obligations.*
- *The archive can be searched for keywords to maintain regulatory compliance.*
- *The archive can be purged of time-ex messages.*
- *The archive can be backed up for further safety.*

Advanced message control and management:

- *Messages can be categorized according to organizational requirements. Examples are OUTMSG, INMSG, SECLVL1 and CONFIDENTIAL.*
- *Message actions can be defined by the administrator according to organizational requirements. Examples are routing of messages, blocking, deleting and copying.*
- *Specific actions can be defined according to combination of message categories. For example, an INMSG with SECLVL1 will be routed to the chief security reviewer.*

Advanced regimen management:

- *The administrator can select the rule-tolerance level at the organization level as well as at the individual level. This determines how strictly and severely the security regimen is implemented.*
- *When a violation occurs, the admin can choose to inform or not to inform the offender of his offense.*
- *When a violation occurs, the admin can choose to allow or not to allow the offender to rectify his error.*



For more information please visit:

WWW.TEXTGUARD.COM