



WHITE PAPER

Getting in Compliance with Government Data Regulations by Leveraging Online Security Technology





CONTENTS

+ Introduction	3
+ Payment Card Industry Data Security Standard (PCI DSS)	4
+ HIPAA	5
+ Sarbanes-Oxley	7
+ FISMA	8
+ Gramm-Leach-Bliley Act	9
+ State Notice of Breach Laws	10
+ Conclusion	10
+ About VeriSign	11



Getting in Compliance with Government Data Regulations by Leveraging Online Security Technology

+ Introduction

The Internet is full of dangers for the unsuspecting and the unprepared. Identity theft and phishing attempts are everyday events—every hour events for some of us, it seems—and the consequences of succumbing can be devastating. To protect vulnerable users from these kinds of attacks, companies such as VeriSign have developed encryption technologies (Secure Sockets Layer or SSL Certificates) for protecting the data that identity thieves crave, especially credit card numbers, payment information, social security numbers, passwords, and confidential personal data. And, since no amount of encryption can protect against a gullible individual giving away prized information to an imposter, the Certificate Authority/Browser Forum, an organization of leading certification authorities (CAs) and vendors of Internet browser software and other applications including VeriSign and others, have also developed another level of technology called Extended Validation (EV) SSL, for providing reassurance that the author of a Web site is indeed who it claims to be.

In the past, it was up to businesses to choose whether to take advantage of these technologies. While many did, some did not—and the consequences fell not only to the victims themselves, but also to institutions that often have to pay directly or indirectly for their mistakes, institutions such as credit card issuers. In order to protect themselves, these institutions, along with governments at various levels and their related standards bodies, have created standards and/or regulations that mandate the use of security and protection technologies in a variety of circumstances. As a result, for institutions naive or careless enough that the danger itself is not a sufficient motivator for using encryption and related technologies, now there is another excellent reason to employ them—because to do otherwise may violate a standard or regulation and risk often-dire consequences.

This white paper explores these standards and regulations—some firmly in place, some emerging, others in the formative stage—and describes the recommendations or requirements they impose for using encryption and related technologies. The reader should bear in mind that this area is a fast-moving target. Today's recommendations are tomorrow's requirements, and new standards are arising all the time. The sooner an enterprise complies, the better positioned it is for the future.



+ Payment Card Industry Data Security Standard (PCI DSS)

There are many ways to steal credit card numbers, but scavenging through garbage cans in search of receipts has given way in recent years to intercepting transmissions between customers making online purchases and their suppliers—a method that is much easier, not to mention cleaner. Since using credit for payment is a very popular way for commerce to be conducted online, the buyer's credit card number must at some point be transmitted electronically to the seller; and if it is unencrypted or inadequately encrypted, stealing it can be easy.

Of the approximately 650,000 complaints about fraud that the U.S. Federal Trade Commission received each year in the period 2004 to 2006, identity theft was the subject a consistent 35% to 36% of the time. 21% of banking institutions have either suffered a security breach during the past two years, or don't if they have. Another 35% have been victims of a phishing attack during the past year.¹ The rampancy of these destructive practices gave rise in years past to a clamor for government regulation of electronic commerce, but the credit card companies that generally had to foot the bill for all the online carelessness felt they could not afford to wait. They knew that SSL Certificates provided the necessary protection for sensitive information and that they can be easily implemented by e-commerce companies and other institutions that transmit and receive credit card information over the Internet. They also knew that without pressure to act, many of these companies would be slow to adopt the technology.

Therefore, in 2005, the world's biggest credit card issuers including MasterCard, Visa, American Express, Discover, and the JCB International Credit Card Company formed a consortium for the purpose of establishing adequate and consistent data security measures that must be used by all merchants, banks, and service providers that store, process, or transmit cardholder data. In 2005 this consortium issued version 1.1 of this set of measures and called it the Payment Card Industry Data Security Standard (PCI DSS). In subsequent years, as both the technology and the thieves became more sophisticated, the consortium enhanced PCI DSS and it is expected to continue doing so for the foreseeable future.

PCI DSS covers many kinds of vulnerabilities that can exist in electronic commerce, and one of its foremost provisions is to require adequate encryption of cardholder data while it is being transmitted. Specifically, it requires strong cryptography such as 128-bit encryption—the minimum level provided by VeriSign Server Gated Cryptography (SGC) SSL Certificates for over 99.9% of site visitors. While this level is considered adequate as of the date of this writing by both PCI and VeriSign, it will not always be sufficient. To future-proof against faster, smarter methods for code cracking, and against tightened restrictions in response by PCI, companies can enable far stronger 256-bit encryption also available from VeriSign and others, depending on the host system operating system and browser used.

¹ State of Information Security Survey 2008 www.bankinfosecurity.com/survey.php



Specifically, PCI DSS requires SGC SSL Certificates for public network Web traffic, SSL VPN for remote access solutions, email encryption (TSL, S/MIME, PGP or desktop-to-desktop) and IPSec VPN to protect payment card information. These requirements apply not only to data in motion but also data at rest in databases, Web servers, and applications that store and/or process credit card data. PCI DSS also requires that crypto keys and their transmissions and storage be effectively managed. While not mandated by the standard, it is also recommended that organizations provide visibility into the SSL traffic to detect threats and employ Web gateway solutions that offer SSL scanning and policy enforcement for encrypted traffic. Finally, for organizations that adhere to the standard by employing adequate encryption, it makes sense to plainly publicize that fact to customers, thieves, and PCI enforcement bodies by prominently displaying widely recognized indicators of the safety of their e-commerce Web sites, such as the VeriSign Secured® Seal.

The credit card companies that comprise PCI are very serious about compliance and have set up rigorous validation processes and penalties for those who breach the standard. While these practices vary somewhat from issuer to issuer, MasterCard's Site Data Protection Plan and Visa's Cardholder Information Security Program are representative. They each require an annual on-site security audit for any merchant that processes more than six million transactions per year or has suffered a security breach that resulted in an account compromise, and for any service provider that processes credit card information or serves as a payment gateway. Other merchants and service providers are required to fill out and submit an annual self-assessment questionnaire in lieu of the on-site audit. In addition, all merchants and service providers must perform a quarterly network scan.

The penalties for violators are severe. They may face higher processing fees or, in more severe cases, can even be barred from using or processing PCI member credit cards at all. In extreme cases, credit card companies issue substantial fines. Visa, for example, levies penalties of up to \$500,000 for each instance of non-compliance while American Express fines merchants up to \$15,000 per day.

Providing protection for credit card information traveling over the Internet has always been a smart practice for the sake of all parties involved. Now, because of PCI DSS, it is not only smart, but mandatory.

+ HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, which affects all health-related organizations in the United States, was originally intended to protect health insurance information when workers changed or lost their jobs. In 2005, in response to the maturation of the Internet as a medium for data interchange, HIPAA expanded its charter and adopted a new set of standards for the electronic maintenance and transmission of protected health information (PHI) – information about the health status, provision of health care, or payment for health care that can be linked to a specific individual. These standards require authentication and authorization controls as well as a minimum 112-bit symmetric encryption and 1024-bit asymmetric encryption of applicable emails, attachments, Web forms, and Web pages to ensure their integrity and make the PHI information they contain undecipherable by anyone other than the intended recipient. HIPAA is administered by the U.S. Department of Health and Human Services.



To assure the security of patient-related data, HIPAA regulations require health plan administrators, healthcare clearinghouses, and healthcare providers to protect and secure any individually-identifiable health-related information including that which is stored or transmitted electronically. To ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI), HIPAA provides a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual. Specifically, health care organizations are required to ensure the confidentiality, integrity, and availability of all electronic protected health care information; to protect against threats to the security or integrity of such information and against unauthorized disclosure or use of protected health care information; and to educate the entire workforce on achieving compliance.

The penalties for violating HIPAA requirements can be quite severe, for example:

- Each instance of unauthorized disclosure by a health care provider is punishable by fines ranging from \$10,000 to \$25,000
- Each instance of intentional unauthorized disclosure is punishable by fines ranging from \$100,000 to \$250,000 and possible jail time
- Although certainly not part of HIPAA itself, the most severe penalty of all might be exposure to lawsuits from the individual whose private medical information is revealed in violation of HIPAA requirements

HIPAA distinguishes between safeguards that are “required” (i.e., must be implemented) and others that are “addressable” (i.e., do not have to be implemented if the organization can document why the specification is not reasonable or appropriate to its circumstances). The data confidentiality safeguard that covers the encryption of data in transit or at rest is in the “addressable” category. The vagueness of the definition of “addressability” has led to considerable disagreement about the criticality of encryption in commonplace practices such as the use of email by doctors to discuss health affairs of their individually identifiable patients. HIPAA requires that the healthcare organization issuing such emails assess its use of open networks, identify the available and appropriate means to protect ePHI as it is transmitted, select a solution, and document the decision. While most experts interpret this requirement to mean that any large healthcare organization should see to it that its emails are encrypted, they disagree about its applicability to smaller organizations and individual healthcare providers.

Those who are uncertain about the applicability of HIPAA’s encryption requirements to themselves should certainly weigh the severity of these penalties, especially the possibility of lawsuits, when reaching a decision. As one expert² claimed, HIPAA could be as lucrative to the legal profession as “asbestos and breast implant litigation combined.” Asbestos and breast implant lawsuits in recent years have resulted in costly settlements and bankrupted companies in both fields.

² New HIPAA security rules could open door to litigation
www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=78684&pageNumber=2

+ Sarbanes-Oxley

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as “Sarbanes-Oxley” or “SOX”, was enacted in response to the flood of headline-dominating financial transgressions by companies such as Enron, Arthur Andersen, and Worldcom that led not only to their downfall but to a serious decline in stock markets and the economic health of the United States. In a nutshell, it was too easy for a company to “cook the books” and for executives to line their pockets at the expense of shareholders while claiming ignorance. SOX greatly tightened restrictions on methods companies can use for maintaining and reporting financial data, and on their financial processes generally. SOX is enforced by the U.S. Securities and Exchange Commission (SEC).

While SOX does not specifically mandate the use of encryption in maintaining or transmitting information, it does require that institutions maintain tight control over access to their sensitive financial data. Some experts³ argue that this requirement implies the need for encryption, since it is the only sure way to remain in control of access even after data is lost or stolen. The SEC could maintain, they feel, that it is bad enough for a company to allow such data to fall into unauthorized hands—but even worse that the company did not take advantage of a readily available technology like encryption to make this information indecipherable.

The Information Technology Governance Institute (ITGI), a group created to assist companies with IT governance, has created a set of security-related recommendations for helping with SOX compliance. One of them is to employ SSL or similar encryption to secure IP connections whenever passwords or other sensitive data may traverse the link. Another is to use digital certificates whenever financial information is moved between systems. While ITGI does not specify a particular level of encryption, it is VeriSign’s opinion that it does not make sense to use anything less than SGC, which enables a minimum of 128-bit encryption for 99.9% of site visitors, when an issue as important as SOX compliance is at stake.

One of the provisions of SOX as an embezzlement preventative is that no single individual in a company should be in position to both make and receive any given payment—a so-called segregation of duties requirement. Therefore it is very important for companies to be able to prove the identity of the author of key communications such as emails that have to do with making or receiving payments, and to be able to state with certainty that they have not been tampered with. Digital signatures are ideal for this purpose.

SOX compliance is a major issue for virtually any publicly traded firm and is the subject of untold numbers of hours spent in company meetings. Its provisions are still not completely understood by many firms, but everyone involved does understand one thing: SOX is very serious business and a breach can lead to detrimental consequences. One of the legislation’s highlights is that CEOs and CFOs must personally vouch for the accuracy of their financial reports, and they can be held personally responsible for non-compliance. Penalties include large fines and jail terms, in addition to damaged public images for them, their employers, and the brand. With consequences this severe and so much ill-defined, many companies are going beyond the letter of the law and incorporating technologies such as strong encryption—such as that offered by SGC technology—that clearly can help demonstrate compliance with the spirit of the law.

One of the criticisms of SOX is that it fails to provide an information security governance framework that corporations can readily adopt to comply with its requirements. In response, to identify such a framework, the Business Software Alliance (BSA) formed an Information Security Governance Task Force which identified ISO 27002 as serving the purpose satisfactorily—heightening the importance of these standards and the use of the encryption and digital signature technologies that they recommend. See below for a description of ISO 27002.

³ When Data Walks: Safeguarding Portable Media <http://www.itcinstitute.com/display.aspx?id=886>

+ FISMA

The Federal Information Security Management Act of 2002 (FISMA) is a U.S. federal government law intended to bolster computer and network security within the government and affiliated parties such as government contractors by mandating yearly audits. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information management systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information contained on RFID tags, which sometimes contains sensitive data, is one major application area.

While not mandating the use of any specific technology, FISMA recommends the use of encryption and digital signature controls to help prevent the loss, modification, or misuse of system data.

Many observers doubt the effectiveness of FISMA as currently constituted, claiming it leads to far more in the way of paperwork than improved security. Consequently there is a move to rewrite many of its key provisions as early as 2008, quite possibly leading to stronger language regarding key security technologies.

FISMA, like SOX, lacks a recommended information security governance framework that corporations can readily adopt. Furthermore, like SOX, the BSA found this need to be adequately fulfilled by the ISO/IEC 27002 standards described below:

ISO/IEC standards

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have issued a series of standards collectively known as “ISO27K” that provide best practice guidance on Information Security Management Systems (ISMS) for protection of confidential information, including the use of encryption. They provide general guidance on the commonly accepted goals of information security management and best practices in the areas of security policy, communications management, and access control, among other subjects.

ISO/IEC 27001 is a certification standard for ISMS, and ISO/IEC 27002 (previously called ISO/IEC 17799) is a standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. They and others comprise ISO27K.

As a set of voluntary international standards, ISO27K recommendations are not enforceable and therefore compliance with the standards themselves is not required. However, they make a number of recommendations on achieving compliance with laws, regulations, contractual obligations, and internal or external security requirements. Their technological recommendations, such as the use of encryption, have been acclaimed for their prudence. As such these recommendations have been adopted as implementation guidelines for complying with other regulations with considerable more direct impact, such as SOX and FISMA.

Since ISO27K has been highly praised and adopted by disparate organizations as their own set of security standards, it makes sense for any security-conscious company to follow its guidelines regarding the use of encryption.

+ Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley (GLB) Act,” is intended to protect consumers’ personal financial information held by financial institutions including banks, securities firms, insurance companies, credit card agencies and other companies that provide services such as lending, brokering, or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; and collecting consumer debts. It covers organizations issuing such personal information as well as those receiving it.

Among the requirements that the GLB Act imposes is the design, implementation, and maintenance of safeguards to protect applicable information. While the GLB Act does not *per se* require that an institution employ encryption as a safeguarding means, it does require them to consider its appropriateness for the purpose and, if it finds encryption to indeed be an appropriate measure, to implement and employ it. Given the value of encryption for safeguarding purposes, it is difficult to conceive of an organization finding it inappropriate. It is therefore easy to imagine a court of law determining that the GLB Act requires encryption for many institutions.

Furthermore, the Federal Financial Institutions Examination Council (FFIEC), a formal interagency body empowered to prescribe uniform principles and standards for the federal examination of financial institutions, recommends the use of encryption to mitigate the risk of the disclosure or alteration of personal financial information and to make sure encryption is of sufficient strength. The FFIEC also has power to investigate institutions and enforce compliance with GLB Act rules, and it expects its recommendations to be followed. If an institution employs weak or no encryption, it carries the burden of demonstrating to the FFIEC that it is nonetheless fulfilling its information safeguarding obligations. It is VeriSign’s opinion that the best way to avoid the possibility of such an accusation is to employ strong encryption, such as that offered by SGC technology.

+ Department of Defense Directive 8100.2

The Department of Defense Directive 8100.2, in effect since 2004, defines mandatory security policies for the use of wireless technologies within the DoD Global Information Grid. Its main purpose is to protect DoD computer networks from the security vulnerabilities introduced via wireless networks. The directive applies to all DoD employees as well as visitors to DoD facilities. It also applies to contractors and others who have access to DoD information.

The directive requires that all data sent to or from wireless devices, as well as all VoIP packets, be encrypted. It also requires that the encryption technology comply with FIPS 140-2 Level 1 or Level 2—which do not specify a particular encryption strength. In addition it specifies that all DoD components ensure that robust, standards-based, FIPS 140-validated authentication and encryption are used in their wireless infrastructure and security technology—including new technologies that emerge in the future.

Finally, it requires that wireless communication not be decrypted at unsecure access points. Experts on this subject⁴ recommend that money allocated to achieving compliance is better spent on a strong overall security solution—clearly including strong encryption—than on shoring up unsecure access points.

⁴ Wi-Fi Technology Forum – Wireless Mobile News and Forums www.wi-fitechnology.com/displayarticle1315.html

+ State Notice of Breach Laws

In addition to the industry standards and federal statutes described above, many states have laws on the books regarding preserving the security of private information about their residents. One such state is California, whose Notice of Breach (previously Senate Bill 1386) law requires that any state agency or California business disclose the breach of security of personal data to any California resident whose unencrypted information was acquired by an unauthorized person. The law covered financial records only until recently, but has now been amended to include medical information as well. Although the law does not mandate encryption, it specifies that only unencrypted information must be disclosed, so organizations that encrypt all private individual information need not worry about breaking this law.

California's law was considered a landmark when it was passed, but has now been met or exceeded by many other states' personal information security statutes. A survey of many of these states' laws reveals that is commonplace if not universal for institutions that employ encryption to be exempted from reporting requirements.

+ Conclusion

Specific levels of encryption are currently required for compliance by two standards organizations, PCI DSS and HIPAA. Others recommend the use of strong encryption and for many companies, these recommendations are effectively iron-clad requirements as well. As technologies and Internet malfeasants alike become ever more sophisticated, governments and institutions are reacting quickly with new laws and regulations for guarding consumer data. Change is the only constant.

Encryption is the most effective and most easily implemented way to help achieve compliance with data privacy and protection regulations. Nearly every federal governing body, including the SEC, FTC, FDA, and NIST, endorses encryption as an information safeguard and, when implemented with sufficient strength, considers it to be an effective demonstration of compliance with their data privacy requirements. No one would argue the sufficiency of SGC, which enables strong encryption for 99.9% of site visitors.

Companies that want to remain competitive with respect to information security in the fast-changing Internet commerce industry have two options. They can attempt to monitor the emergence of new laws and standards, and meet each new requirement as it arrives with a technological response – a difficult undertaking to say the least. Or they can choose now to adopt the strongest practical level of protection for their customers and other constituents that technology makes available – strong encryption accompanied by extended validation. This approach will allow them to be confident that ample protection is in place for a long time to come. With SGC, every site visitor can experience the strongest SSL encryption available to them, and with EV they have equal assurance that they are helping to protect their customers to the maximum extent possible from falling victim to phishing attacks. For more information about EV and SGC, please visit our SSL information center at: <http://www.verisign.com/ssl/ssl-information-center/index.html>.



+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.Verisign.com for more information.

This paper does not render legal advice or opinion. The standards and law in the areas of privacy and security continues to evolve, and may be subject to local, state, or federal regulation. VeriSign and its subsidiaries make no guarantee about the legal accuracy of the information provided in this paper. All users and organizations seeking legal advice should secure the services of a competent legal professional.

©2008 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

00026065 5-29-2008