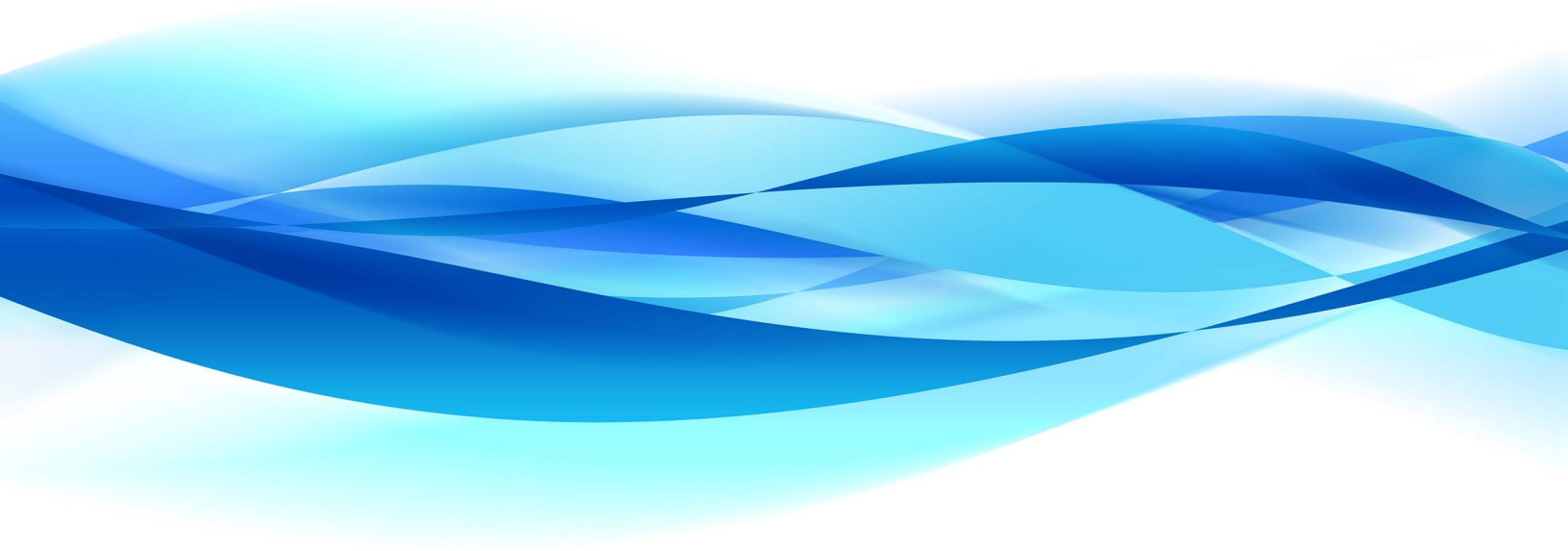
NeoCertified

Whitepaper



THE CASE FOR SECURE EMAIL

by Peter J. Schaub

The Case for Secure Email

By Peter J. Schaub, NeoCertified™

In our increasingly digitalized and fast-paced world, email has become a necessary means of communication for individuals, businesses, educational institutions and government agencies. It's estimated that nearly 205 billion emails are sent each da. That's nearly 2.5 million emails each second and 76 trillion per year: that number is expected to exceed 100 trillion emails annually in the coming years. However, with the convenience and speed of email comes the risk that messages can be intercepted and private information can be compromised. With the number, and sophistication, of hackers increasing, companies need to take proper precautions to safeguard confidential information. According to Sophos, an IT Security firm, only 44% of 1,700 organizations surveyed in their private independent study extensively use encryption to secure their data. The number of high-profile data breaches in recent years illustrates the seriousness of this issue.

Identity theft is rapidly becoming one of the most common crimes in America. One of the primary ways identity theft occurs is through the interception of emails. With email increasingly becoming the method of choice for individuals and institutions to communicate and send information, the interception of emails can lead to the compromise of sensitive company or client information that can be used to perpetrate fraudulent activities. The effects of fraud and identity theft can be highly damaging, not only personally and financially, but also for the security and reputation of a business or institution.

While there are numerous solutions to enhance the security of email, the most simple and effective method is to encrypt the email and its attachments with the use of a password. Both the sender of the email and its recipient use a predetermined password to encrypt the email before it is sent and de-encrypt the email upon receiving it. Once the sender has used a password to send an encrypted email, the recipient of the email will then use a password to de-encrypt the email and its attachments. By encrypting the email and its contents when the message is sent, the sender mitigates the risk of the email being compromised through interception, and the recipient can have confidence that the message was sent in a secure manner.

With those considerations in mind, there are five primary reasons to utilize a secure email service or product:

I. To meet Federal & state-level legal and regulatory requirements for:
- **a) The Financial Services Industry**
- **b) The Healthcare Industry**
- **c) The Legal Industry**
- **d) Publically Traded Companies**
- **e) Those subject to State-specific laws**

II. **To provide the highest level of confidentiality for employee and clients' privileged data.**
III. **To obtain legally-binding documentation of the receipt of a message.**
IV. **To get a message to a recipient in the quickest manner possible.**
V. **To reduce costs, as opposed to utilizing regular or express mail for signed documents.**

Each of these areas is briefly described below:

I. **<u>To meet federal and state-level legal and regulatory requirements</u>**.

In general, these laws simply require that you keep all privilege or Non-Public Information (NPI), like social security number or account numbers and passwords, secured when the data is transmitted or stored electronically. Based on your industry, there could be several laws applicable to you.

a. <u>Financial Services Industry</u>

1. For banking and other financial services-related areas, one of the big issues is the email correspondence between organizations and their boards of directors. How severe would the consequences be to the organization if those emails were intercepted? Beyond just the business consequences, there are several legal aspects. According to the Gramm-Leach-Bliley Act's (GLBA) privacy provisions, corporate officers are subject to the financial-institution section of the act. Specifically, Section 6801 of the GLBA, and section 501(b), requires financial institutions to have the "administrative, technical and physical safeguards" to protect the security and confidentiality of their client records by May, 2003, including email communications. A fine of $10,000 per infraction can be charged for noncompliance with the law. In addition, financial institutions are required to comply with the Federal Financial Institutions Examination Council Guide requirements for securing sensitive information in storage and in transit. See Section "A.1" for a more specific description of the GLBA regulation and the FFIEC Guide requirements.

   Any business (publicly or privately held) that maintains or possesses consumer information must protect all privileged data as per the Fair and Accurate Credit Transactions Act (FACTA) requirements. Please see Section "A.5" for more specific information about the law. Another relevant regulation as related to financial institutions is from Federal Financial Institutions Examination Council (FFIEC) which states that a financial institution should use encryption to mitigate the disclosure of sensitive information in storage and at rest. Section "A.4" for more detailed description of the requirement.

2. Pertaining to the Securities & Brokerage industry, there are multiple laws and regulations governing the securing of privileged and confidential data. Specifically, the Security and Exchange Commission (SEC) rules, SEC 17a-3 & 17a-4, and the National Association of Security Dealers (NASD) rules require not only that the privileged or NPI data be secure in transit and at rest, the data must be retained for auditing purposes for specified periods of time; – both online and backed-up. Please see Section "A.3" – SEC & NASD for more specific details regarding these requirements.

   Additionally, the Securities & Brokerage industry has the FINRA requirements for the handling of NPI. Specifically, the rule requires that when information is provided on a portable media device, it must be encrypted. The data must be encoded into a form in which the meaning cannot be assigned without the use of a confidential process or key. Please Section "A.6" for specific details of the FINRA requirement.

b. Healthcare Industry

Another industry that requires significant data protection is the Healthcare industry, which is dealing with the enforcement of HIPAA (the Health Insurance Portability & Accountability Act of 1996). How an individual's information is sent, controlled and audited is addressed in the Title II section of HIPAA. This section of HIPAA states that anyone who has access to a person's individually identifiable health information, including all administrative and financial information that is in electronic form, whether it is stored or transmitted, is subject to HIPAA's security standards. The intent of these standards is to protect the confidentiality and integrity of "individually identifiable health information," past, present or future. Failure to meet these requirements results in severe civil and criminal penalties, including fines up to $25,000 for multiple violations in a calendar year and fines up to $250,000 and/or imprisonment up to 10 years. See Section "B" for a more specific description of the HIPAA regulation.

c. Legal Industry

In 1998, the American Bar Association issued an extensive opinion (Formal Opinion 99-413 dated 3/10/1998) approving email as a confidential and privileged means of communication, as required by the legal community's Model Rule 1.6. This rule requires that communications by US Lawyers be governed by the ethical obligation to protect confidential client information. However, with the recent rash of lawsuits and government inquiries as a result of emails, many lawyers are questioning the ability of email to provide a confidential and privileged means of communications. See Section "C" for a more specific description of the Model Rule 1.6 requirement. Additionally, if lawyers are corresponding with their clients regarding financially-related data or a financial transaction, they may be

also subject the GLBA regulations as well. See Section "A.1" for a more specific description of the GLBA regulations.

d. Publically Traded Companies

All publically-traded companies are subject to the Sarbanes-Oxley Act of 2004. The Sarbanes-Oxley Act was passed in response to numerous scandals occurring in the late 1990s and the beginning of the 21st century including companies such as Enron, WorldCom, and Global Crossing. In addition to its other provisions (changing the responsibilities of board members and increasing penalties for white-collar crimes), the law requires all publicly-traded companies to provide an annual report as to their internal control structures. While there has been substantial discussion about what is required for an "adequate control structure" for a publicly-held firm, there should be little doubt that a secure electronic mail system is critical to achieving that goal. Please see Section "A.2" SARBOX for more specific details on the law.

e. State-specific laws

Regardless of your industry, there are many states that have general laws that apply to all organizations, public and private, for-profit and non-profit. Basically, the state laws, which include but are not limited to California, Nevada, Illinois and Massachusetts, all require that all Non-Public Information (NPI) must be secure in transit and at rest. For some of the specific laws by state, please see Section "D", State Laws.

II. Provide the highest level of confidentiality for employees and clients.

The most serious problem with traditional email is the ease of which email can be intercepted and used in criminal activity. With just basic information about an email user, a person with criminal intent can find free software on the Internet that would allow them to intercept almost anyone's email. Once an email has been intercepted, a hacker can interfere with the email communication in four ways:

- **a.** Eavesdropping - Where the information remains intact but its privacy is compromised.
- **b.** Tampering - Changing the contents of the email and then sending the email on to the intended recipient.
- **c.** Impersonation *(spoofing)* - Someone pretending to be you.
- **d.** Misrepresentation - Someone orders items using your credit card or using your social security number to obtain credit.

III. Provide legally-binding documentation of receipt of a message.

For the same reason that people use Certified Mail by the USPS to document the receipt of a letter by someone, users of secure email can document the date and time a recipient

receives and opens their secure email thus providing legally binding documentation of receipt. With many secure email systems, the sender can see the exact date and time (down to the second) of when a message was sent, as well as opened by the intended recipient. And with systems that have Digital Signature abilities, the sender can verify that the message had not been intercepted and no one but the intended recipient opened the message. This is often referred to as the "registered" email process.

IV. To get a message to a recipient in the quickest manner possible.

While regular USPS mail can take several days or express mail can take 24 hours, secure email can be sent and received by a recipient within minutes. Now with the acceptance of Electronic Signatures sent via email, the cost of sending legally-signed documents is reduced dramatically. (Please note, Digital Signatures and Electronic Signatures are not the same, and in most states, Digital Signatures are not accepted as legal signatures; only Electronic-Signatures are accepted as legal signatures on a document in those states.)

V. Save money as opposed to regular or express mail.

When you send a regular letter, it costs the time to print, address, and mail the letter. Postage alone can easily exceed a dollar per letter. Sending via express mail, it can cost up to $12.00 per letter and $20 for a small set of documents. So for example, if you sent 20 letters a month and 10 express packages, it would cost approximately $224 per month where secure email can cost as little as $50 per month, saving $170 dollars per month or $2000+ per year!

C. CONCLUSION:

One way, and probably the easiest way, for business and healthcare professionals to meet their legal and regulatory requirements is to encrypt email communications through a secure messaging product, such as NeoCertified™. NeoCertified™ allows the sender to easily encrypt email messages and attachments and only the intended recipient can decrypt the message.

The bottom line is that email has become a significant part of both our personal and business lives, and to be able to communicate effectively and quickly, we must be aware of the risks of using email. In order to prevent our emails from being intercepted, we must either implement some form of protection (NeoCertified™) or choose not to send emails that contain personal information. Either we do that or we simply need to accept the possibility of paying significant fines, compromising our clients' and employees' personal data or reading the contents of your emails on the front page of the morning newspaper…. Your choice.

Peter Schaub is the President and founder of NeoCertified, LLC, a leading provider of secure email services since 2002. Their website is www.neocertified.com and he can be contacted at peter@neocertified.com.

SECTION "A" FINANCIAL INSITITUTIONS

1. GLBA

Formal Name: Gramm-Leach-Bliley Financial Services Modernization Act
Common Name: Gramm-Leach-Bliley Act or simply GLBA or GLB
Statute Number: Public Law 106-102
Law Applies To: All Financial Institutions (Publicly-held and Privately-held) as well as professionals (lawyers, accountants) that work with financial institutions
Penalties for Non-compliance: Civil penalties up to $100,000 per violation, plus possible sanctions, including but not limited to termination of FDIC insurance and management removal Provision Requiring Email Security: GLBA 501(b) codified at 15 USC§ 6801

Exact Text:
In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805 (a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
(1) To insure the security and confidentiality of customer records and information;
(2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Explanation of Law and how it applies:
The Gramm-Leach-Bliley Act (referred to as GLBA) is best known to the outside world as the law that repealed portions of the Glass-Steagall Act, which for almost 70 years had banned combining commercial and investment banking. In banking circles, however, GLBA is best known for section 501 (b) of the act, which requires financial institutions to properly safeguard customer records and information. Under the law and its accompanying regulations, all financial institutions must maintain tight security on the personal financial information of their customers. This includes any personal information that is included in emails. Financial institutions must have specific policies and programs to protect the financial and personal information contained in emails.

http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

2. SARBANES-OXLEY (SARBOX)

Formal Name: Public Company Accounting Reform and Investor Protection Act of 2002
Common Name: Sarbanes-Oxley Act or simply SARBOX or SOX
Statute Number: Public Law 107-1204
Law Applies to: Publicly held companies
Penalties for Non-compliance: SEC can levy fines and for severe violations of SARBOX criminal punishments (including prison) are possible
Provision Requiring Email Security: Section 404 (a)

Exact Text:

— RULES REQUIRED —

(1) The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall — state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Explanation of law and how it applies:
The Sarbanes-Oxley Act was passed in response to numerous scandals occurring in the late 1990s and the beginning of the 21st century including companies such as Enron, WorldCom, and Global Crossing. In addition to its other provisions (changing the responsibilities of board members and increasing penalties for white-collar crimes), the law requires all publicly-traded companies to provide an annual report as to their internal control structures. While there has been substantial discussion about what is required for an "adequate control structure" for a publicly-held firm, there should be little doubt that a secure electronic mail system is critical to achieving that goal.

3. SEC and NASD RULES

Statute Number: Securities and Exchange Commission Rules 17a-3 & 17a-4 and National Association of Securities Dealers Rules 3010 & 3110. Law Applies to: All firms and individuals (publicly- held and privately-held) that deal with securities.

Penalties for Non-compliance: Penalties can be assessed for up to millions of dollars. In 2002, the SEC fined several large Wall Street firms for failing to retain emails.
Provision Requiring Email Security: Rules 17a-3, 17a-4, 3010, 3110.

Exact Text:

a. Review of Correspondence

Each member shall develop written procedures that are appropriate to its business, size, structure, and customers for the review of incoming and outgoing written (i.e., non-electronic) and electronic correspondence with the public relating to its investment banking or securities business, including procedures to review incoming, written correspondence directed to registered representatives and related to the member's investment banking or securities business to properly identify and handle customer complaints and to ensure that customer funds and securities are handled in accordance with firm procedures. Where such procedures for the review of correspondence do not require review of all correspondence prior to use or distribution, they must include provision for the education and training of associated persons as to the firm's procedures governing correspondence; documentation of such education and training; and surveillance and follow-up to ensure that such procedures are implemented and adhered to.

(3) Retention of Correspondence
Each member shall retain correspondence of registered representatives relating to its investment banking or securities business in accordance with Rule 3110. The names of the persons who prepared outgoing correspondence and who reviewed the correspondence shall be ascertainable from the retained records and the retained records shall be readily available to the Association, upon request.

Explanation of Law and how it applies:
The SEC, NASD, and stock exchanges are extremely serious about the maintenance of all correspondence with clients, including all electronic correspondence. It is an absolute requirement that firms dealing with securities have a safe, dependable, secure, and easily accessible email program.

FDIC

http://www.fdic.gov/news/news/financial/2001/fil0168.html
http://www.fdic.gov/news/news/financial/2001/fil0168a.html
http://www.fdic.gov/news/news/financial/2007/fil07105a.pdf
http://www.fdic.gov/news/news/financial/2007/fil07105.html

4. FFIEC

In 2006, the Federal Financial Institutions Examination Council (FFIEC) released a handbook on information security practices. Regarding encryption, it stated that financial institutions should use encryption to mitigate the use of disclosure or alteration of sensitive information in storage and transit. Encryption should include:

1. Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk
2. Effective key management practices
3. Robust reliability

4. Appropriate protection of the encrypted communication's endpoints
For more information, go to:
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

5. FACTA

Formal Name: Fair and Accurate Credit Transactions Act
Common Name: FACTA or FACT Act
Statute Number: Public Law 108-159
Law Applies to: Any business (publicly held or privately held) that maintains or possesses consumer information
Penalties for Non-compliance: Both state and federal governments can levy fines for non-compliance. Additionally, any consumer harmed by failure to comply may bring a civil action to recover for any damages caused by the non-compliance.
Provision requiring email security: FTC regulation listed at 16 CFR Part 682

Exact Text:

(a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by Taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
(b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

Explanation of Law and how it applies:
The Fair and Accurate Credit Transactions Act provides ways for consumers to deal with credit reports and receive one free credit report annually. In addition, it protects consumers from fraud by requiring that businesses properly dispose of any consumer information. This includes any consumer information contained in emails. It is critical to have an email system that allows proper disposal of all emails.

6. FINRA - 8210

The SEC approved amendments to FINRA Rule 8210 (Provision of Information and Testimony and Inspection and Copying of Books) that require information provided via a portable media device pursuant to a request under the rule be encrypted, as described in more detail below.

a. These amendments take effect on December 29, 2010. FINRA Rule 8210 confers on FINRA staff the authority to compel a member firm, person associated with a member firm or other person over which FINRA has jurisdiction, to produce documents, provide testimony or supply Regulatory Notice 10-59 November 2010 written responses or electronic data in connection with an investigation, complaint, examination or adjudicatory proceeding.

b. FINRA Rule 8210(c) provides that a firm's or person's failure to provide information or testimony or to permit an inspection and copying of books, records or accounts is a violation of the rule. Frequently, member firms and persons that respond to requests pursuant to FINRA Rule 8210 provide information in electronic format. Because of the size of the electronic files, often this information is provided in electronic format using a portable media device such as a CD-ROM, DVD or portable hard drive.

c. In many instances, the response contains personal information that, if accessed by an unauthorized person, could be used inappropriately.

d. Data security issues regarding personal information have become increasingly important in recent years.

e. In this regard, FINRA believes that requiring persons to encrypt information on portable media devices provided to FINRA in response to Rule8210 requests will help ensure that personal information is protected from improper use by unauthorized third parties. As amended, the rule requires that when information responsive to a request pursuant to Rule 8210 is provided on a portable media device, it must be "encrypted"—i.e., the data must be encoded into a form in which meaning cannot be assigned without the use of a confidential process or key. To help ensure that encrypted information is secure, persons providing encrypted information to FINRA via a portable media device are required:
(1) to use an encryption method that meets industry standards for strong encryption; and
(2) to provide FINRA staff with the confidential process or key regarding the encryption in a communication separate from the encrypted information itself (e.g., a separate email, fax or letter).

Currently, FINRA views industry standards for strong encryption to be 256-bit or higher encryption. Encryption software meeting this standard is widely available as embedded options in desktop applications and through various vendors via the Internet at no cost or minimal cost to the user.

For more information, go to
http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p122487.pdf

Section "B" HealthCare

1. HIPAA

Formal Name: Health Insurance Portability and Accountability Act
Common Name: HIPAA
Statute Number: Public Law 104-191
Law Applies to: Health plans (individual or group plans that provide or pay for health care, including employer plans), health care clearinghouses, and health care providers. Applies to all firms whether publically held or privately held.
Penalties For Non-compliance: Civil penalties of up to $10,000 per violation
Provision Requiring Email Security: HHS regulations implementing HIPAA listed at 45 C.F.R. § 164.306(a).

Exact Text:
Subpart
C—Security Standards for the Protection of Electronic Protected Health Information
(a) General requirements. Covered entities must do the following:
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4). Ensure compliance with this subpart by its workforce.

Explanation of Law and how it applies:
HIPAA was created to deal with continuing legal issues involving health insurance. The law also set very tight boundaries for the protection of health information. The Health and Human Services Department regulations implementing the law emphasize both privacy of health information and security of health information. Secure email systems are important for maintaining both privacy and security.

Section "C" Legal

1. ABA Legal Rules

Formal Name: American Bar Association Model Rules of Professional Conduct – Client-Lawyer Relationship Rule 1.6 Confidentiality of Information
Common Name: Attorney-Client Confidentiality Rules
Law Applies to: All attorneys both public and private
Penalties for Non-compliance: State bar sanctions, fines, potential malpractice claims
Provision Requiring Email Security: ABA Rule 1.6

Exact Text:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

Explanation of Rule and how it applies:
Under Rule 1.6, an attorney has a duty to protect all confidential information of his or her clients. While there is no absolute duty to use encrypted emails for client communications, an attorney must provide reasonable safeguards based upon the sensitivity of the client's information. Additionally, having a secure email system will often be very attractive to clients.
NOTE: In certain circumstances, attorneys may also be required to meet standards under HIPAA or GLBA.

Section "D" State Laws

In addition to the federal laws listed above, States are beginning to require email encryption on transfers of personal customer information. Nevada is one of the first states to pass a statute requiring email encryption. As an example of what these new state laws are like, here is the exact language from the new Nevada statute (NRS 597.970):

A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business, unless the business uses encryption to ensure the security of electronic transmission.

The State of Nevada passed a law in October 2008 that all businesses, no matter how small or what they do, must secure confidential customer information if it is sent electronically. Statute 597.970 states that any form of Internet communication, including via Web sites and email, must encrypt personal data. To learn more, click on: http://www.leg.state.nv.us/Nrs/NRS-597.html#NRS597Sec970 and

http://online.wsj.com/article/SB122411532152538495.html

The Commonwealth of Massachusetts has mandated that, effective January 1, 2010; companies are required to encrypt all personal information of state residents transmitted electronically or wirelessly. This includes Social Security and employer identification numbers, drivers' license or identity card data, account, credit and debit card numbers with any password or security and access codes. For more background, go to: http://www.mass.gov/?pageID=ocapressrelease&