

**AMAX White Paper**

**Solutions for Protecting  
Data in Transit: Insuriti™  
Secure and Bonded/Insured  
Transmissions**

**November 2006**

---

## Solutions for Protecting Data in Transit: Insuriti Secure and Bonded/Insured Transmissions

©AMAX Consulting, LLC 2006  
Legal Content Contributed by  
Daniel J. Langin<sup>1</sup>

### Introduction

Companies spend significant effort securing data in storage, but do little to protect data in transit. This tendency to focus on data *at rest* is changing, however, due to numerous laws, regulations and standards that require companies to protect sensitive data *while it is in transit*. The Sarbanes-Oxley Act, the PCI data security standard, the Gramm-Leach-Bliley Act, FTC Section 5A and the Health Insurance Portability & Accountability Act (“HIPAA”) require companies to protect data in transit. Under these provisions, companies that fail to secure data in transit face civil suits, fines and sanctions.

### What is Data In Transit?

Data in transit includes: (a) data on all types of removable physical media such as tapes, discs, or flash drives, being physically transported to offsite facilities, and; (b) data transmitted electronically either within a company’s network or from the company to third parties. Because some very high-profile losses of data being physically shipped occurred in 2002 and 2003, an increasing amount of data is now transmitted electronically. This paper will use the term “data in transit” to mean sensitive data electronically transmitted within a company’s network and to third parties.

Is data in transit usually secure? Recent losses suggest that it is not 100% secure.

### Losses of Data In Transit

Most data in transit losses are probably underreported based on fear of negative publicity and loss of share value<sup>2</sup>. At least one study found that reporting of security incidents actually correlates with a loss in share value<sup>3</sup>. Accordingly, reports of data in transit losses are few, but the losses are significant.

The most recent high profile data in transit loss concerned BJ’s Wholesale Club. According to an action filed by the FTC (see discussion of FTC Section 5A below), BJ’s “fail[ed] to encrypt consumer information when it was transmitted or stored on computers in BJ’s stores.” Identity thieves intercepted this information and made millions of dollars in unauthorized purchases, resulting in an estimated \$13 million in civil claims against BJ’s.

The BJ’s incident may be the tip of the iceberg. A 2003 survey by Zix Corporation sampled 4.4 million e-mails sent by 7500 healthcare organizations in a one-week period, and determined that 4%--or 176,000 messages--contained unencrypted PHI (a violation of HIPAA, with penalties starting at \$1000 per day). If this survey indicates the volume of unsecured data in transit, then companies have a lot to worry about under the laws, regulations and standards described below.

---

<sup>1</sup> Principal of Daniel J. Langin, Attorney at Law, LLC. Dan has over 17 years of experience including thirteen years in technology, business law and intellectual property litigation and counseling. See [www.langinlaw.com](http://www.langinlaw.com) or contact Daniel at (913) 661-2430 or [dlangin@langinlaw.com](mailto:dlangin@langinlaw.com). This article is provided for educational and informational purposes, not as legal advice.

<sup>2</sup> See, for example, 2005 CSI/FBI Survey at 20 (figure 22) (most common reason that companies do not report incidents to law enforcement is negative publicity/loss of stock value).

<sup>3</sup> See *id.* at 20, fn. 5.

### ***Sarbanes-Oxley Act (“SOX”)***

SOX focuses on corporate accounting and financial reporting, not data security. However, compliance with SOX involves data security because most companies’ financial reporting processes depend so heavily on information technology. SOX sections 302 and 404 are the most pertinent to data in transit.

Section 302 requires the CEO and CFO of a publicly-traded company to certify in annual and quarterly reports to the SEC that they are “responsible for establishing and maintaining internal controls” to ensure that material financial information is accurately reported to them<sup>4</sup>. Because so much reporting depends on e-mail, companies may be required to ensure that data for financial reporting is transmitted securely.

Under Section 404, internal controls must also include policies and procedures that provide “[r]easonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on financial statements<sup>5</sup>.” Because many companies’ assets are tied up in information assets that are often shared by e-mail or other means of transmission, procedures that protect data in transit may be needed for 404 compliance. A July 2004 PWC study, in fact, identified a lack of automated controls and excess human intervention as a major SOX compliance barrier<sup>6</sup>.

### ***Gramm-Leach-Bliley Act (“GLBA”)***

GLBA applies to all businesses that collect or maintain consumer financial information, including banks, thrifts, collection agencies, retailers that extend credit and so forth<sup>7</sup>. GLBA applies, among other things, to any systems used to transmit customer information.<sup>8</sup>

GLBA requires the protection of data in transit. GLBA regulations (Interagency Guidelines<sup>9</sup> and NCUA Guidelines<sup>10</sup>) require institutions to place controls on systems (including those used to transmit customer information) to prevent customer information from being sent to unauthorized parties<sup>11</sup>. This is important because “phishing” attacks commonly involve a financial institution insider who sends information to an identity thief. The same section requires institutions to consider “[e]ncryption of electronic customer information, *including while in transit . . .*” (emphasis added)<sup>12</sup>.

GLBA sanctions can be significant. For example, the FDIC may impose fines ranging from \$5,000 per day up to \$1,000,000, and may use noncompliance in determining safety and soundness of the institution.

<sup>4</sup>Sarbanes—Oxley Act section 302 (a)(4)(B); Marks, “Director, Trustee and Officer Liability for Information Security,” available at [www.dwt.com](http://www.dwt.com) (2003).

<sup>5</sup> 68 Federal Register 36636, 36640, June 18, 2003.

<sup>6</sup> Price-Waterhouse-Coopers, “New Reporting and Compliance Rules Challenge Systems at Most Large U.S. Companies” (July 2004).

<sup>7</sup> Under 15 USC Section 6809.(3), a financial institution is “any institution the business of which is engaging in financial activities,” which under 12 USC Section 1843(k) includes lending, investing, insuring and providing financial, investment or related services.

<sup>8</sup> These systems are defined by regulation as “customer information systems” “member information systems” or “information security programs. See, e.g. 66 Federal Register 8635 (Interagency Guidelines), 68 Federal Register 479589 (draft Interagency Guidance).

<sup>9</sup> Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of the Year 2000 Standards for Safety and Soundness, 66 Federal Register 8616-8641 (February 1, 2001).

<sup>10</sup> Standards for Safeguarding Customer Information, 67 Federal Register 36484-494 (May 23, 2002).

<sup>11</sup> Interagency Guidelines Section III.C.1.a.

<sup>12</sup> Interagency Guidelines Section III.C.1.c.

### ***FTC Section 5A and State Attorneys General Actions***

Businesses face the risk of fines and penalties under FTC Section 5A (unfair and deceptive trade practices) or similar state laws for failing to protect customer data. In the recent FTC action against ChoicePoint, the company was fined \$10 million in civil penalties and forced to pay \$5 million in consumer redress because its employees were duped into sending personal financial records of over 160,000 consumers to phony “subscribers” who requested them<sup>13</sup>. As noted above, the FTC sanctioned BJ’s WholeSale Club in 2005 for “failing to encrypt consumer information when it was transmitted or stored on computers in BJ’s stores,” resulting in millions of fraudulent charges. BJ’s agreed to 20 years of monitored security by the FTC, and faced an estimated \$13 million in civil claims.

State attorneys general (AGs) have used state unfair trade practice laws to pursue the same claims as the FTC. Ziff Davis Media,<sup>14</sup> Victoria’s Secret<sup>15</sup> and other companies have been required to pay five- and six-figure fines to state AGs for failing to secure customer data and violating their own privacy policies.

The common thread in each of these regulatory actions is a company’s failure to meet basic information security standards, including protection of data in transit. Fines have *increased* over time, culminating in the \$15 million ChoicePoint fine, the largest in FTC history.

### ***HIPAA***

HIPAA<sup>16</sup> governs collection, use and security of consumer health information (“PHI” - protected health information). HIPAA applies to doctors and hospitals, payors and health data processors (collectively “Covered Entities”). One of the hidden facts about HIPAA is that it applies to the group health plan operations of most employers<sup>17</sup>. Because so many employees now work at home or use mobile computing devices to work remotely, and so much medical transcription data is sent overseas, securing health data in transit is an increasing problem.

The HIPAA Security Rule’s “Transmission Security” section states that Covered Entities must “[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.<sup>18</sup> Commentary to this section notes that the need to protect data is much greater when PHI is transmitted over the Internet<sup>19</sup>.

---

<sup>13</sup> See <http://www.ftc.gov/opa/2006/01/choicepoint.htm>

<sup>14</sup> Hale & Dorr, “Data Security Gains Attention from Regulators and Private Claimants,” May 30, 2003 ([www.haledorr.com](http://www.haledorr.com)).

<sup>15</sup> *Id.*

<sup>16</sup> 42 U.S.C. Sections 1171-79.

<sup>17</sup> Employee group health plans that are totally self-insured, self-administered and have under 50 participants are not covered.

<sup>18</sup> Section 164.312(e)(1).

<sup>19</sup> *Id.* at 8357.

### ***The PCI Data Security Standard (“PCI”)***

In addition to laws and regulations, companies face compliance requirements in private industry standards. Visa, in collaboration with several other major credit card brands, created the PCI (Payment Card Industry) Data Security Standard. All merchants and service providers that handle, transmit, store or process credit cardholder information or related data were required to be PCI compliant as of June 30, 2005.

Requirement 4 of PCI requires companies to “safeguard sensitive cardholder data during transmission over public networks” by encryption and other means. Although PCI refers to SSL, SSL is not necessarily a complete solution to data in transit risks (see discussion below).

Non-compliance with PCI comes with a hefty price tag. Fines of up to \$500,000 per incident can be assessed by the card brands if a non-PCI-compliant entity is compromised, and failure to immediately report a suspected or known loss or theft of data can result in \$100,000 fines per incident. PCI noncompliance can also result in a merchant’s worst nightmare: suspension or revocation of its right to accept or process credit card transactions.

### ***Risk Management and Protecting IP in Transit***

Even if a company is not subject to these laws, regulations or standards, it must consider protection of data in transit from a risk management point of view. Companies readily send their and their customers’ most sensitive data and intellectual assets over the Internet without protection. But what happens if it is lost? Most technology vendors disclaim responsibility or limit liability for lost data, and companies usually do not insure it. The 2005 CSI/FBI Survey suggests that *only 25% of information security risks are insured*<sup>20</sup>. Furthermore, most of these insurance policies (even if they cover data in transit) do not cover data in transit *once it leaves the company’s network*.

In the same way that a prudent company would not think of shipping goods without protection, it must consider how to protect its data and intellectual assets in transit. Officers and directors are required to act as reasonably prudent persons to protect a company’s interests, and many of the laws and regulations identified in this paper (especially SOX and GLBA) put compliance responsibility directly on a company’s board of directors or C-level officers.

---

<sup>20</sup> 2005 CSI/FBI Survey at 10 (figure 12)

**Insuriti -- Patented Processes****Systems and methods for insuring data transmissions****Abstract:**

Systems and methods are provided which afford a technical application for insuring, bonding, and underwriting a transmission of a data set, streaming data, and/or document over the Internet through TCP/IP and all other electronic media such as WAP (wireless application protocol), VOIP (voice-over IP), fiber optic channels, microwave channels, and through standard electrical switches, electrical outlets and power lines. The present invention includes a computer readable medium having computer executable instruction to cause a system perform a method for insuring, bonding, and/or underwriting data transmission. The method includes enabling a first remote client coupled to a communications network to insure, bond, and/or underwrite a transmission of an electronic data set, streaming data, and/or document, with a selected coverage type for a selected coverage amount, from the first remote client to one or more second remote clients. The method further includes charging a fee to an appropriate account for the selected coverage type and amount.

***The Need for a Complete Solution: Technical Protection and Management/Transfer of Risk***

Few good solutions exist to address protection of data in transit. Digital certificates address the beginning and end of transmissions (authenticating user, sender or site), but not the middle, while secure protocols such as SSL or VPN permit secure transmission, but do not authenticate the user. Furthermore, technical solutions alone are not enough: *None* of these solutions include financial recourse in the event of a loss.

A truly robust solution would therefore combine technical protection of data in transit with a risk management and risk transfer component to create financial recourse in case data in transit is lost.

***Conclusion: Insuriti™ Secure and Bonded/Insured Transmission Patents Support Robust Solutions***

Solutions can be created based on the Insuriti™ patents for bonding/insuring and securing data in transit. Licensing these patents can enable companies to build solutions that meet compliance requirements and mitigate or transfer risk for data in transit. The holder of these patents is prepared to license them to companies that wish to develop processes to send and receive secure and bonded/insured data transmissions. Such licensees may be able to build the cost of the program into the costs it passes on to its customers or business partners, thus essentially allowing the license to pay for itself.

Using a secure and bonded/insured transmission process makes good legal and risk management sense. As the volume of online transmissions of sensitive data increases, Congress and the states will pass more laws regulating data in transit. A scalable process for securing data transmissions and providing financial recourse if they fail will solve an entire range of problems for companies that transmit their customers' and their own sensitive data electronically.

---

***For additional information, please contact:***

Al Stern  
AMAX Consulting, LLC  
[al.stern@amaxconsulting.com](mailto:al.stern@amaxconsulting.com)

612-743-9696