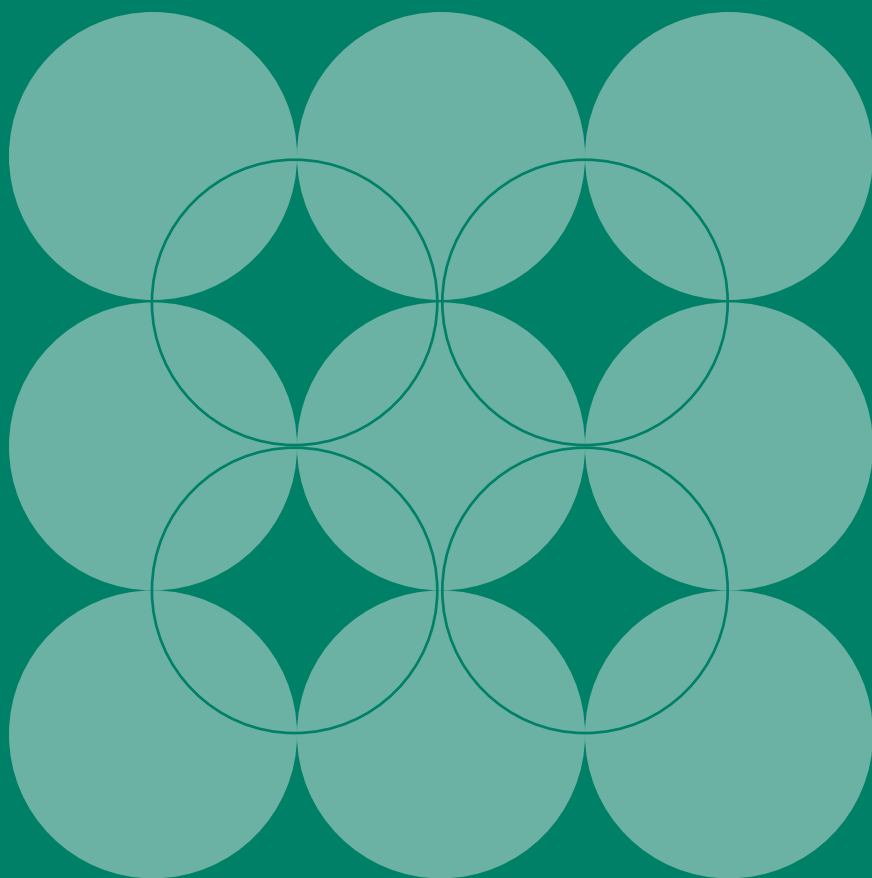


# Protecting Personal Information: The Good, the Bad, the Ugly



A White Paper Commissioned by:  
**MBA Board of Directors  
Technology Steering  
Committee**

# PROTECTING PERSONAL INFORMATION: THE GOOD, THE BAD, THE UGLY

A white paper commissioned by the  
MBA Board of Directors Technology Steering Committee

The information provided is educational in nature, providing general information about legal developments and is not intended as legal advice. You should consult an attorney for any specific legal questions.

## INTRODUCTION

The MBA Board of Directors Technology Steering Committee (BoDTech) serves as the primary advisory body to MBA's Board of Directors on technology matters. This security white paper is in response of a request by the MBA Board of Directors to raise the awareness within industry as it relates to personal information protection.

The rise of the Internet and internet-related technologies in the latter half of the 1990s and into the new millennium has changed, and continues to change how companies, organizations and agencies conduct their business. Namely, the Internet and its related technologies have enabled organizations to:

1. Become more operationally efficient
2. Reduce long-term operational costs
3. Increase revenue and profits
4. Increase connectivity and outreach to customers
5. More quickly develop new services and products for customers
6. More quickly deliver services and products to customers

What is worth noting is the relationship between items 1-3 (namely *company benefits*) and items 4-6 (namely *customer benefits*). Specifically, the better a company is at implementing capabilities that increase outreach to customers (4), more quickly develop new services and products (5), and more quickly deliver those services and products (6), the more likely that company is to increase operational efficiencies (1), reduce operational cost (2), and increase revenues and profits (3). Figure 1 depicts this relationship.

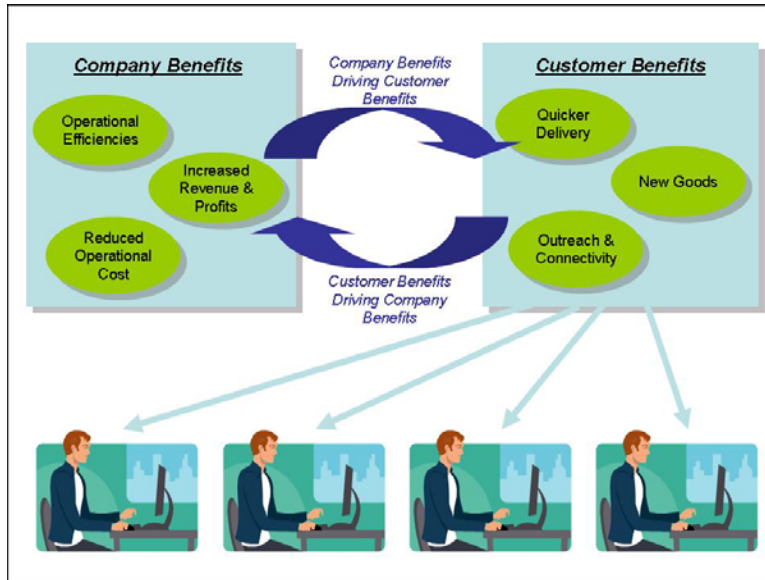


Figure 1

A core component for providing *customer benefits* is the collection and processing of customer information. However, as a company collects, aggregates and processes more customer information, and specifically personal information (PI) such as social security numbers, credit card numbers, etc., that company needs to recognize its obligations for protecting PI and retaining customer confidence in that company, and the correlation those obligations have with a company's overall reputation of being a trusted provider of Internet-based services.

Unfortunately, as reported multiple times in the press this year<sup>1</sup>, companies have found themselves being negatively publicized in the headlines of newspapers and publications for mismanaging and disclosing PI in an unauthorized manner. More than ever, the information explosion, aided by an era of easy credit, has led to the expansion of a crime that feeds on the inability of consumers to control who has access to their PI and how it is safeguarded. That crime is identity theft.<sup>2</sup>

The security breaches relating to PI that were publicized this year have brought much needed attention to safeguarding PI. While legislation has already existed that requires some amount of protection for PI, such as the Gramm-Leach-Bliley (GLB) Act<sup>3</sup> and the Health Insurance Portability and Accountability Act (HIPAA),<sup>4</sup> it was the Security Breach and Notification Law of California (CA SB 1386)<sup>5</sup> that proved to be the catalyst, as this law required businesses to notify consumers whose PI had been breached and potentially compromised. Several states have followed California's model and enacted their own legislation<sup>6</sup>, and the Federal Government is likely to enact similar legislation at

<sup>1</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

<sup>2</sup> From the Identity Theft Resource Center web site: <http://www.idtheftcenter.org/facts.shtml>.

<sup>3</sup> <http://banking.senate.gov/conf/confprpt.htm>.

<sup>4</sup> <http://www.cms.hhs.gov/hipaa/>.

<sup>5</sup> [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

<sup>6</sup> <http://www.pirg.org/consumer/credit/statelaws.htm#breach>.

the national level.<sup>7</sup> With legislation paving the way, companies are now realizing the importance for having the reputation of being a *trustworthy* provider of Internet-based goods and services, which includes the secure management of PI. Revenue and profit are no longer the sole drivers of *company benefits*; being a *trustworthy* company is becoming just as important. *Trust* is a benefit mutually shared by company and customer, and it provides a bridge between traditional *company benefits* and *customer benefits*, thereby providing balance between company and customer needs. For the purposes of this whitepaper, the use of the term “trust” does not denote a fiduciary responsibility. Figure 2 depicts the evolving Internet-based environment between company and customer.

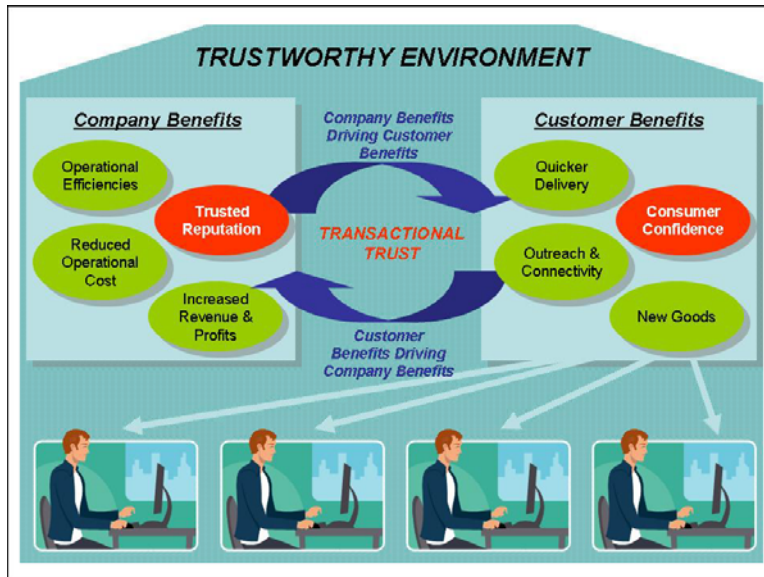


Figure 2

With the mortgage industry being one of the biggest collectors and processors of PI, it is critical that all institutions involved in our business begin embracing the *trustworthy* environment depicted in Figure 2. Reputation and consumer confidence need to be added to the lists of *company* and *customer benefits*, respectively. As an industry that is involved in one of the biggest transactions an individual ever makes in his/her life (i.e., purchasing a home), trust is a critical element in gaining and retaining the confidence of that individual.

The remainder of this paper discusses in more detail the importance for mortgage industry institutions to safeguard PI, the implications for doing so and not doing so, and recommended actions an organization can take in ensuring the protection of PI. Mortgage institutions can also leverage the recommendations made in this paper to protect other types of sensitive information such as employee PI and internal confidential information. These are all types of critical information assets that should be safeguarded within an organization.

<sup>7</sup> [http://www.epic.org/privacy/bill\\_track.html](http://www.epic.org/privacy/bill_track.html).

## PROTECTING PI...THE GOOD

Consumers assume a certain level of trust with their Internet-based service providers (e.g., banks, retailers). Namely, consumers assume the information they are providing about themselves to support an electronic transaction is being carefully managed and protected. This level of trust comes from the consumer looking for the “padlock icon” in his/her web browser, which signifies a Secure Sockets Layer (SSL)<sup>8</sup> connection has been established between the consumer’s web browser and the company’s web site to support the secure transfer of the consumer’s PI. What consumers didn’t understand (until the well-publicized security breaches occurred in early 2005) is that many companies did little to protect the PI once it was originally provided by the consumer, or collected through other means (e.g., business partners, data aggregators). Figure 3 depicts this un-trusted environment.

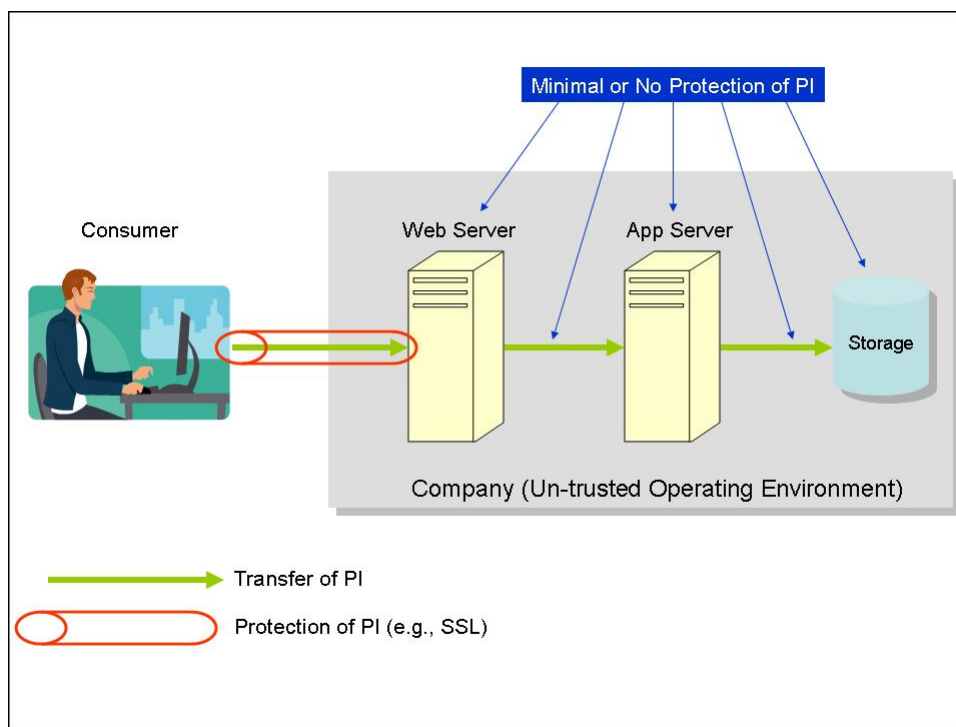


Figure 3

In a 12 month period, roughly 7 million people became victims of identity theft as reported in two 2003 studies by Gartner Research and Harris Interactive. That equals 19,178 victims per day, 799 victims per hour, or 13.3 victims per minute. Based on a study performed by the Identity Theft Resource Center, the business community loses between \$40,000 - \$92,000 per name in fraudulent charges. In addition, approximately 85% of victims found out about the crime due to an adverse situation (e.g., denied credit or employment, notification by police or collection agencies, receipt of credit cards or

<sup>8</sup> SSL is the de facto standard for encrypting data between a web browser and a web server.

bills never ordered). Only 15% found out through a positive action taken by a business group that verified a submitted application or a reported change of address.<sup>9</sup>

What is alarming about these statistics is that the typical consumer and business are unaware, and have been unaware of the magnitude of the identity theft problem. However, with laws such as CA SB 1386 that require consumer notification when their PI may have been breached, consumers and businesses are becoming quickly educated with the growing problem of identity theft.

News reports of major security breaches with companies such as ChoicePoint,<sup>10</sup> Citigroup,<sup>11</sup> Bank of America,<sup>12</sup> and CardSystems,<sup>13</sup> have caused consumers (including US Senators) to become more cautious about how their PI is managed and distributed. These types of breaches may lessen the amount of overall trust that consumers have in executing electronic transactions. To regain that trust, companies need to be proactive in identifying and protecting PI. As important as it was to implement SSL to protect the initial transfer of PI from consumer to company and gain consumer confidence in Internet-based transactions, companies now need to take further steps in protecting PI. To ensure the safeguarding of PI throughout workflow processes and the entire operating environment, organizations should:

- Implement security policies and procedures based on industry standards and best practices
- Execute those security policies and procedures on a daily basis
- Employ security technologies that protect PI throughout the lifecycle of an electronic transaction
- Employ and appropriately train personnel operating in trusted roles.

Please see Figure 4 for an illustration of these recommendations.

In the identity theft space identity thieves will move to new environments when their efforts are thwarted. What is considered now to be a growing problem with the credit card industry and the stealing of personal information that includes credit card numbers, may well become a problem for the mortgage industry and services supporting mortgage instruments such as Home Equity Lines of Credit (HELOCs). As the credit card industry combats the identity thieves and implements additional protections for PI, identity thieves will look for other insecure, high volume environments where they can gain financially using stolen PI. The issuance of HELOCs can provide such an environment for identity thieves because of the ease to obtain a HELOC if PI is known, as well as the high volume of HELOCs that are processed and approved each year.

---

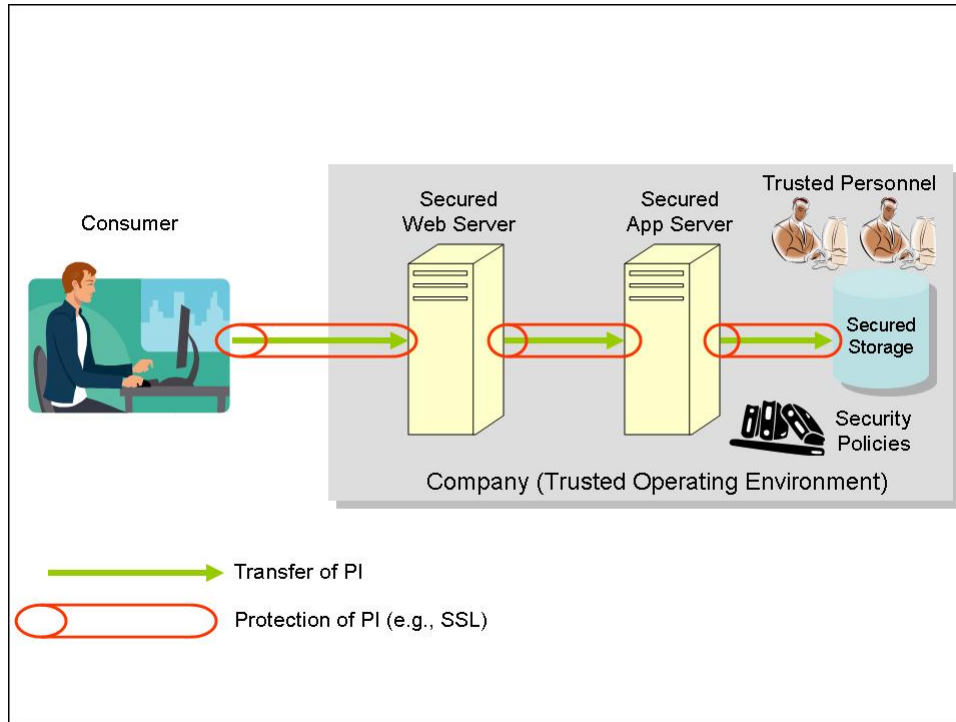
<sup>9</sup> <http://www.idtheftcenter.org/facts.shtml>.

<sup>10</sup> <http://www.epic.org/privacy/choicepoint/>.

<sup>11</sup> [http://money.cnn.com/2005/06/06/news/fortune500/security\\_citigroup/](http://money.cnn.com/2005/06/06/news/fortune500/security_citigroup/).

<sup>12</sup> <http://www.msnbc.msn.com/id/7032779/>.

<sup>13</sup> [http://money.cnn.com/2005/06/17/news/master\\_card/](http://money.cnn.com/2005/06/17/news/master_card/).



**Figure 4**

PI needs to be considered a critical information asset that requires protection within every mortgage company. Therefore, PI needs to be identified, assessed in terms of risks, and safeguarded accordingly. The Mortgage Industry Standards and Maintenance Organization (MISMO) Information Security Working Group (ISWG) is developing a set of recommendations and best practices (based on recognized industry standards) for protecting PI within certain mortgage industry institutions. They have categorized five (5) general use cases for PI that can be applied to any mortgage entity: collecting PI, processing PI, transferring PI, storing PI and disposing PI. Figure 5 summarizes these five general use cases.

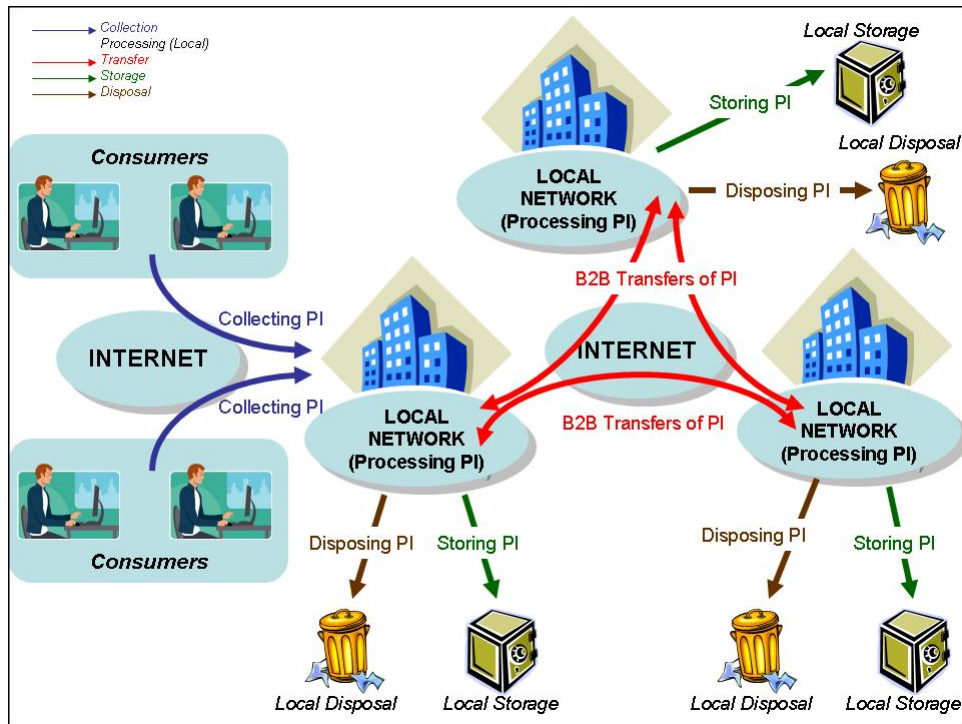


Figure 5

Figure 5 comes directly out of the ISWG’s Best Practices Guidelines for Personal Information Protection,<sup>14</sup> and it defines a notional, web-based environment that any mortgage entity can leverage in assessing its own PI protection requirements. By understanding one’s own working boundaries (i.e., the local network defined in Figure 5), one can then begin to assess how and where PI is collected, processed, transferred to other entities, stored (locally or non-locally), and disposed. Upon assessment, organizations will be better prepared to implement security solutions that provide appropriate protection of PI.

For example, Figure 5 shows that organizations have a responsibility to continue to safeguard PI as it is transferred between organizations. If an organization engages third party service providers to execute certain mortgage related processes, then that organization should ensure their service providers are also protecting PI commensurate with the organization’s own PI protection requirements.

For mortgage entities that embrace these recommendations to identify, assess and protect PI, those entities will prove over time that they are reputable and trustworthy providers of *customer benefits* to their consumer bases. Trust and reputation are key factors in a company’s relationship with its customers, and as that trust and reputation become enhanced over time, the *company’s benefits* will be enhanced as well.

<sup>14</sup> The MISMO ISWG Best Practices Guidelines for Personal Information Protection is presently being developed.

## NOT PROTECTING PI...THE BAD

Referring back to Figure 4, implementation of security technologies, policies, procedures, and trusted personnel requires investment and continuing maintenance by a company. Therefore, trade-offs need to be performed to determine “how much security” is “enough security” to adequately protect PI. Unfortunately, companies that only focus on perimeter security (i.e. security at the “walls” of the company such as an Internet firewall or a physical lock on a door) to provide an “appearance of security” are still faced with security issues within the organization. The result is that many points exist within the organization where PI is exposed in unprotected form. See Figure 6.

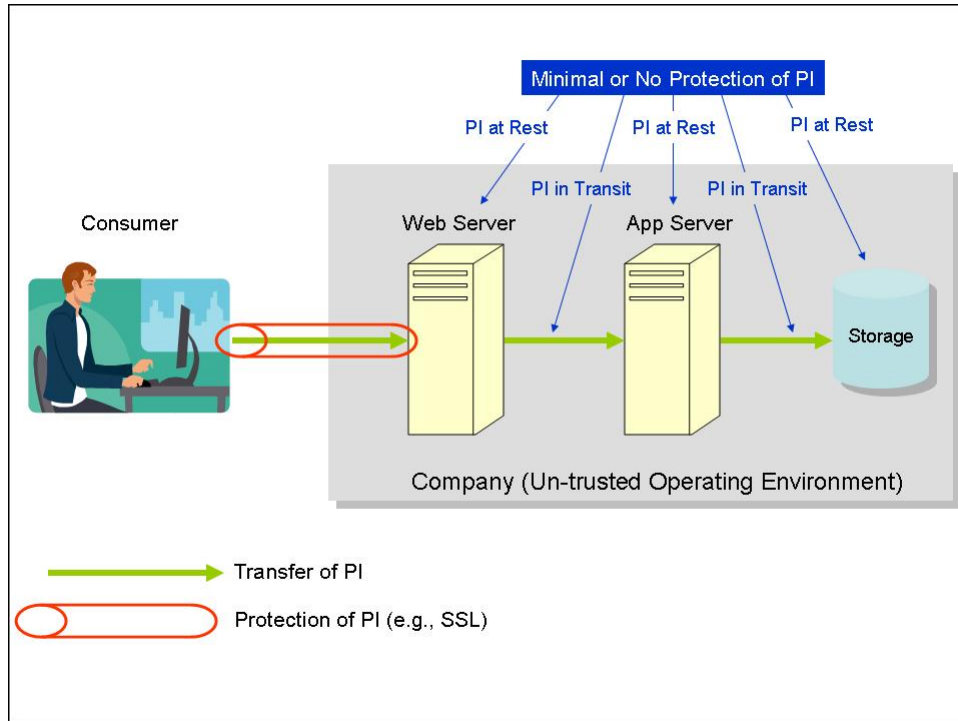


Figure 6

To emphasize this further, on September 28, 2005 the Federal Trade Commission (FTC) announced a settlement with Superior Mortgage Corporation.<sup>15</sup> The FTC disputed Superior’s claims that the PI was protected. Superior used SSL to encrypt data over a public network (i.e., from the customer web browser to Superior’s web server), but it failed to safeguard PI that traversed through its corporate offices. Superior’s broad statement of PI protection did not match the reality of their business process.

Should an unauthorized individual gain access to that unprotected PI (whether in transit or at rest), certain risks arise both for the consumer and the company. Consumer risks include delay or disruption in customer services, and more seriously identity fraud. This can lead to many other consumer risks (e.g., illegal purchases and poor credit scores, which lead to turn downs for loans). Company risks also include delay or disruption in

<sup>15</sup> <http://www.ftc.gov/opa/2005/09/superior.htm>.

customer services (which lead to operational inefficiencies and increased operational costs), as well as fallouts from consumer risks – namely the processing of illegal transactions (e.g., bad loans). Given the high volume, automated environment for processing of items such as home equity loans and lines of credit, a significant security breach of PI could cause major financial damage to a mortgage organization.

Imagine the following examples:

- An unauthorized individual completes hundreds or thousands of on-line applications in the names of people whose PI has been stolen. Even if a small percentage of those applications are processed and approved, the resulting financial damage would be large.
- An insider threat (employee) sells PI to a competitor who then uses the PI to gain customer market share. Or, the employee sells the PI for his/her own financial gain to a third party operating a “black market” operation involving the selling and trading of PI to those desiring to perform identity theft acts.
- Individuals set up what is believed to be a legitimate business, and gain access to PI that is resident within a major aggregator of PI whose job it is to provide such information to legitimate businesses.
- A foreign student studying in the United States builds a credit history while in the United States, and then sells his/her PI upon completing school and leaving the country.

These are not only examples regarding the unauthorized access and use of PI, they are real-world scenarios that have occurred and continue to occur. Are these security trade-offs worth considering when determining “how much security” is “enough security” in protecting PI? Is your company willing to stake its reputation and risk being highlighted on the front page of a newspaper because it was involved in a security breach regarding the disclosure of PI?

Companies tend to think that protecting PI is more of a benefit for the consumer rather than the company. Therefore, when it comes to making trade-off decisions regarding the level of protection for PI, companies have an easier time justifying the implementation of a lax security solution in order to keep costs down. However, the examples above show that protection of PI is not just a *customer benefit*, but a *company benefit* as well. Specifically, a company’s reputation is enhanced when it is viewed as being a protector of PI and a promoter of consumer confidence in Internet-based transactions. As that reputation is enhanced, consumers gain more confidence in doing business with that company over the Internet, which leads to growth in the more traditional *company benefits*. Furthermore, securing PI within an organization can mitigate fraud, gain competitive advantages, reduce reputation risk associated with consumer notification laws (and specifically, non-compliance with those laws), and more important, improve the trusted relationship with customers.

Figure 6 reinforces the need for a mortgage company to identify PI as a critical information asset that needs to be securely managed. It is not just the asset of the consumer; it is also the asset of the company. Ask yourself these questions:

- What is your company plan for performing security trade-offs in determining the appropriate level of protection for PI?
- Have you assessed which of the five general use cases shown in Figure 5 apply to your organization?
- Have you examined the ISWG's recommendations for protecting personal information to assist in defining applicable threats and vulnerabilities related to PI, as well as recommended technologies, policies and procedures to protect your organization against those threats and vulnerabilities?

Failure to identify, assess and protect PI can result in significant deterioration of *company* and *customer benefits*, as shown in the examples above. Failure to even acknowledge the importance of protecting PI within your organization can be catastrophic, as we discuss in the next section.

## NOT PROTECTING PI...THE UGLY

One of the worst things that can happen to any company is to appear in the press as having performed something illegally or having made a negligent error that causes harm to many parties. News of this stature typically erodes consumer trust in the company and can potentially have significant impact on the company's financial status (e.g., drop in stock price). Furthermore, law suits and fines may arise from such advertised activities that further damage a company's reputation and financial standings.

Table 1 highlights events that occurred for some companies and organizations in 2005 regarding the unauthorized disclosure of PI.<sup>16</sup> Some industry estimates indicate that over 50 million identities have been affected.

**Table 1**

Company	Event	No. of People Affected
ChoicePoint	Accessed by ID Thieves	145,000
Bank Of America (BofA)	Lost Backup Tape	1,200,000
Lexis Nexis	Passwords Compromised	312,000
CardSystems	Hacking	40,000,000
CitiFinancial	Lost BackupTapes	3,900,000
FDIC	Not Disclosed	6,000
University of California Berkley	Stolen Laptop	98,400
University of Hawaii	Dishonest Insider	150,000
DSW/ Retail Ventures	Hacking	Additional 1,300,000

There apparently were deficiencies on the part of these companies to fully identify, assess and protect PI. Furthermore, it appears that security trade-offs involving the level of protection for PI did not consider the risks related to public exposure of security breaches and incidents. Now these companies are struggling to secure their business and technical processes,<sup>17</sup> regain the trust of their customers and business partners,<sup>18</sup> improve the financial standing in the public marketplace,<sup>19</sup> and respond to Governmental inquiries dealing with security breach legislation.<sup>20</sup>

<sup>16</sup> A full listing of companies suffering security breaches related to PI can be found at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

<sup>17</sup> [http://www.choicepoint.com/news/statement\\_050405\\_1.html](http://www.choicepoint.com/news/statement_050405_1.html).

<sup>18</sup> <http://www.theregister.co.uk/2005/07/19/cardsystems/>.

<sup>19</sup> <http://www.techweb.com/wire/security/171200329>.

<sup>20</sup> [http://www.onlinesecurity.com/individual/page386\\_2.php](http://www.onlinesecurity.com/individual/page386_2.php).

You can start to gauge where your organization stands in the “Good-Bad-Ugly” spectrum in protecting PI by answering the following questions:

- Are you proactively working to understand applicable legislation,<sup>21</sup> and what your legal requirements are for safeguarding PI, as well as notifying parties when a potential security breach of PI has occurred?
- Are you assessing your organizational boundaries as they relate to the collection, processing, transfer, storage and disposal of PI?
- Are you focusing on the identification, assessment and protection of PI within your organization?
- Are you performing thoughtful security trade-offs that include the balancing of *company benefits* and *customer benefits*?
- Are you concerned about your reputation as a trustworthy business entity, or are you more concerned about your company’s own bottom-line numbers?
- Are you making appropriate investments in protecting PI, or are you willing to risk the disclosure of your customers’ PI and the consequences that result from that disclosure (e.g., bad press, falling stock prices)?

As a mortgage entity, trust and reputation are your fundamental discriminators between you and your competitors. For the average citizens going through a mortgage process, they have little knowledge for how their PI is managed. They do assume though that it is being managed carefully and securely, until they read about security breaches in the press. Which path will your organization choose? The *Good* Path; the *Bad* Path; or the *Ugly* Path? Perhaps Table 2 may be a guide in helping you answer this critical question for you organization.

---

<sup>21</sup> The MISMO ISWG Best Practices Guidelines for Personal Information Protection is presently being developed.

**Table 2**

<b>The Path You're On...</b>	<b>...If You're Doing This</b>
Good	Acknowledging that PI is a Critical Information Asset Being Proactive in Protecting PI Understanding Legislative Implications for Protecting PI Identifying, Assessing and Protecting PI Performing Security Trade-Offs that Balance Customer and Company Benefits Understanding that Solutions Involve Technology, Processes and People Referencing ISWG's Guidance and Recommendations for Solution Implementations
Bad	Performing Minimal Activities to Meet Imposed Requirements for Protecting PI (e.g., passing audits) Being Reactive in Protecting PI Performing Security Trade-Offs that Provide more Company Benefits over Customer Benefits Not Leveraging Recommended Practices and Standards
Ugly	Paying No Attention to the Protection of PI Believing that Your Organization will not Incur a Security Breach Involving PI Not Recognizing the Importance of Trust and Reputation in the Internet-based Marketplace Believing that Solutions are Only Technical Solutions Believing that Browser Security (e.g., SSL) is "Good Enough" Security

## STEPS YOUR ORGANIZATION CAN TAKE

For reasons noted throughout this whitepaper, organizations should take steps to protect PI data. The biggest step your organization can take is acknowledging that PI is a critical information asset, and that it needs to be managed and secured like any other critical information asset within your organization. Secondly, every organization needs to understand that a solution for securing PI is not solely a technical solution, but one that involves people and processes as well. The MISMO ISWG has been promoting a general five-step security method<sup>22</sup> in all of its security activities. This same five-step method, which is consistent with ISO 17799,<sup>23</sup> can be used by any mortgage institution to identify, assess and safeguard PI. This method is also useful in performing activities required to comply with industry regulations such as the Federal Trade Commission (FTC) Safeguards Rule,<sup>24</sup> as well as the various State legislations addressing notification requirements for security breaches involving disclosure of PI. In summary, this method involves:

- *Business and Risk Description* – Simply stated, the risk is not protecting PI and the ramifications for not protecting PI that are discussed in this paper. Business descriptions are use cases specific to your organization where PI is handled. The ISWG has generally described these use cases as collecting, processing, transferring, storing and disposing PI. Mortgage companies should use these general use cases to identify in more detail the PI use cases that are specific to their environment, where environment is defined as the physical environment (e.g., buildings, offices), the logical environment (e.g., networks), and the legal environment (e.g., security breach notification laws, consumer protection laws, required security audits). The result of this activity is a detailed understanding of where PI exists and how it should be handled accordingly within your company.
- *Policy and Architecture* – This is the foundation for protecting PI within your organization. The policy defines the high level requirements for securely managing PI, and in the case where a breach occurs, for providing appropriate notification to the required entities (e.g., consumers, company officers, , authentication, authorization). The architecture is the framework for implementing specific technical and procedural solutions in support of your company’s policy (e.g., segregation of responsibilities and infrastructure, interconnectivity).
- *People, Processes and Technology* – These are the detailed specifications for your organization to comply with your policy and to be implemented in accordance with your architecture. People need to be informed and trained on requirements for handling PI; processes need to be put in place to ensure every individual and computer operates correctly with respect to the handling of PI; and technology

---

<sup>22</sup> The 5-step security method comes from A&N Associates, Inc.’s Information Assurance Solution Development Method. This method has been provided to MISMO under MISMO’s IPR policy, and is available to any mortgage entity.

<sup>23</sup> ISO 17799 is an international standard defining a comprehensive set of controls comprising best practices in information security.

<sup>24</sup> This rule requires financial institutions under FTC jurisdiction to secure customer records and information. See <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

needs to be selected and implemented that provides the appropriate level of PI security (e.g., encryption, access control, auditing, intrusion detection, anti-virus, regulatory compliance).

- *Support Plan* – Identity theft and the notification of security breaches is an evolving landscape. Your organization should identify individuals who have a responsibility to keep up with this changing landscape (e.g., new laws, new identity theft tactics, new security technologies and best practices). By keeping up with the changing landscape, your organization can adapt quickly and implement new solutions (or enhance existing solutions) for protecting PI. Business Continuity Plan/Disaster Recovery (BCP/DR), and maintenance plans (including change control) are elements of a Support Plan.
- *Education* – Education and awareness may be the single most important program your organization performs regarding the protection of PI. The more your management, employees, contractors, etc. understand the importance of PI and the reputation benefits that can be gained by being an advocator of protected PI, the more successful your organization will be in implementing PI security solutions.

If your company already has a dedicated and knowledgeable security team, encourage them to embrace the 5-step method above, as well as monitor or become involved with the activities of the ISWG with respect to protecting PI. If your company needs consultation services, there are many organizations (large and small) that can assist your company through the 5-step method above. Companies with expertise in or offering ISO 17799 compliance services are good candidates. It is highly recommended that you clearly define your initiative as protecting PI with a strict emphasis on notification requirements, and you should ensure that any consultants you hire are able to tailor their services appropriately.

For additional information pertinent to this paper, please visit:

<https://sharepoint.mismo.org/default.aspx> (MISMO Information Security Working Group – Requires Account Access)

<http://www.sisac.org/> (MBA Secure Identity Services Accreditation Corporation)

<http://www.privacy.ca.gov/recommendations/secbreach.pdf> (Recommended Practices on Notification of Security Breach Involving Personal Information)

<http://www.idtheftcenter.org> (Identity Theft Resource Center)

<http://www.privacyrights.org/ar/ChronDataBreaches.htm> (Privacy Rights Clearinghouse)

<http://www.epic.org> (Electronic Privacy Information Center)

<http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm> (FTC Safeguard Recommendations for GLB)

<http://www.ftc.gov/opa/2005/09/superior.htm> (FTC Settlement with a Mortgage Company over its Information Security Practices)

## **ABOUT THE AUTHORS**

R.J. Schlecht is an Industry Technology Director for Security and Compliance at the MBA. He has 20 years of network and information security experience. His primary responsibility with the MBA has been logical authentication and identity management.

[rschlect@mortgagebankers.org](mailto:rschlect@mortgagebankers.org)

202-557-2843

[www.mortgagebankers.org](http://www.mortgagebankers.org)

Yuriy Dzambasow is a Principal Consultant with A&N Associates, Inc. – a small business specializing in Information Assurance (IA) consulting services. He has 15 years of IA experience, with a focus in Public Key Infrastructure (PKI) and identity management.

[yuriy@anassoc.com](mailto:yuriy@anassoc.com)

410-859-5449 x107

[www.anassoc.com](http://www.anassoc.com)