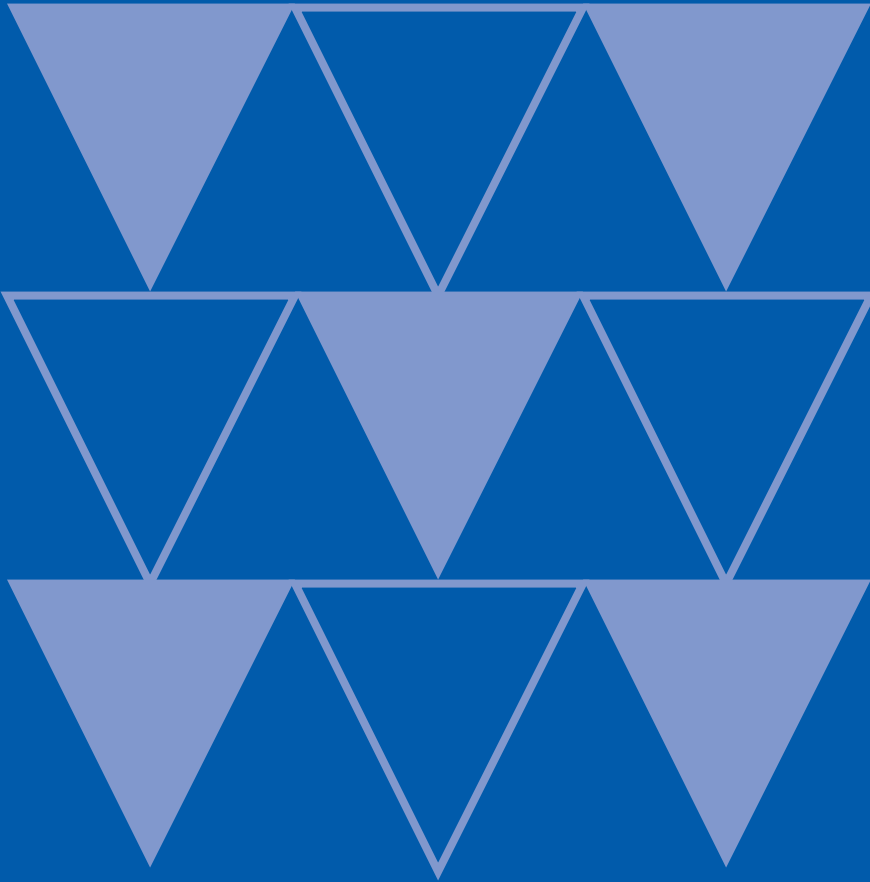


# Identifying and Safeguarding Personal Information:

**Recommended Guidelines and Practices**



**MISMO Information  
Security Work Group**



This paper is published by the Mortgage Industry Standards Maintenance Organization, Inc. (“MISMO®”), a wholly owned subsidiary of the Mortgage Bankers Association, and is a mortgage industry reference tool, providing voluntary guidelines to facilitate efficient eMortgage processes and reduce cost, time, and risks. **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.**

MISMO® is a registered service mark of the Mortgage Bankers Association.

© 2005 Mortgage Industry Standards Maintenance Organization, Inc. All rights reserved.

***Revision History:***

<b>Issue</b>	<b>Date</b>	<b>Change History</b>
1.5	7/5/05	RJS/MBA – Generalize introduction for generic State privacy personal privacy protection guidelines.
1.6	8/8/05	RJS/MBA – Replace “prevention” with “protection” and move CA SB 1386 narrative into State Legislation section.
1.7	8/22/05	RJS/MBA – Change section 3 from a Business functional description to a data oriented risk analysis. Yuriy Dzambasow/A&N Assoc. – Draft section 3.
1.8	10/10/05	RJS/MBA – Update State Legislation sub-section 2.5 and replace Guidelines section 3 with updated outline.
1.9	11/16/05	MBA Legal review
2.0	12/5/05	RJS/MBA – Review legal comments and integrate ISWG solicited comments.
2.1	12/14/05	RJS/MBA – Updated section 3 per comments received from ISWG.
2.2	12/19/05	RJS/MBA – Legal review modifications
2.3	1/6/06	RJS/MBA – Review updates

1.	Introduction.....	4
1.1	State Legislation.....	4
1.2	Scope.....	4
1.3	Purpose of Guidelines.....	5
2.	State Legislation.....	5
2.1.	CA SB 1386 Overview .....	5
2.2	CA SB 1386.....	6
2.2.1	Personal Information.....	6
2.2.2	Unauthorized Access .....	7
2.2.3	Encryption Safe Harbor .....	7
2.3	Privacy Protection White Paper .....	7
2.4	Other States Legislation.....	8
2.4.1	Introduction.....	8
2.4.2	Idiosyncrasies of Bills.....	8
2.4.3	Personal Information Identified in State Legislation .....	10
3.	Guidelines for Safeguarding Personal Information .....	10
3.1.	Analysis of PI Use Cases – Threats, Vulnerabilities & Risks .....	13
3.1.1	Collection of Personal Information.....	13
3.1.1.1.	Definition .....	13
3.1.1.2.	Threats and Vulnerabilities .....	13
3.1.2.	Processing of Personal Information .....	16
3.1.2.1.	Definition .....	16
3.1.2.2.	Threats and Vulnerabilities .....	16
3.1.3.	B2B Transferring of Personal Information .....	20
3.1.3.1.	Definition .....	20
3.1.3.2.	Threats and Vulnerabilities .....	20
3.1.4.	Storing Personal Information.....	24
3.1.4.1.	Definition .....	24
3.1.4.2.	Threats and Vulnerabilities .....	25
3.1.5.	Disposing Personal Information .....	29
3.1.5.1.	Definition .....	29
3.1.5.2.	Threats and Vulnerabilities .....	29
3.2.	Recommended Policies and Procedures .....	33
3.3.	Recommended Security Technologies.....	37
3.4.	Recommended Incident Response Plans .....	40
3.4.1.	Incident Monitoring and Notification .....	41
3.4.2.	Impact Assessment.....	41
3.4.3.	Internal Notification.....	42
3.4.4.	External Notification.....	43
3.4.5.	Follow-Up Assessment .....	44
4.	References.....	46
Exhibit A.....		48
	State Legislation Data Element Matrix.....	48

# 1. Introduction

The Internet and distributed technology have created risks associated with the unauthorized disclosure of personal information that have not been historically experienced. Today's Internet-driven business environment enables unlimited availability to services for customers, employees, and partners, and unfortunately many organizations adopted Internet-based solutions driven by revenue or cost reduction without due consideration to personal information protection.

Recently, the protection of personal information has become a major concern to both the private and public sectors. The public sector – Federal, State, and Local governments – is starting to regulate privacy. Gramm-Leach-Bliley Act (GLBA), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) and Sarbanes-Oxley Act are examples of federal regulations. State governments in Arkansas, California, Connecticut, Florida, Georgia, Illinois, Maine, Montana, North Carolina, North Dakota, and Washington have all codified similar laws requiring organizations to disclose information related to security breaches within those organizations. Many other States are following suit and enacting similar legislation.

The MISMO Information Security Work Group (ISWG) has drafted guideline recommendations for protection of State legislated individuals' personal information. This white paper identifies personal information data elements specified by States outlines data use case applicable to the mortgage industry, and reference recommended security practices for policy technology and security incident response.

## 1.1 State Legislation

The unfortunate fact is that any guidelines attempting to fully define State legislation in the area of personal information is an exercise in futility. States are moving at record pace adopting laws governing the protection and notification of unauthorized access to information. These privacy regulations concern paper or computerized media and plain text or encrypted data. Compounding the issue is an expanded definition of classified personal information by States and the lack of a federal regulation for some form of consistency.

There is however some generic analysis that can be conducted on the States' regulatory activities and generalized guidelines proposed for the protection of personal information. The ISWG used the California Senate Bill (CA SB) 1386 as the model for the analysis. The CA SB 1386 Law on Notification of Security Breach has been used by other States and the proposed Federal government as well. As additional States enacted privacy legislation, an evaluation was performed and content added to the white paper.

## 1.2 Scope

The objective of this paper is to identify and recommend guidelines to prevent the unauthorized disclosure of personal information as identified by breach notification legislation. Additionally, the scope of this paper is limited to computerized personal information. Breaches notification, credit freeze, and other mandated requirements of notification legislation are outside the scope of this document. Data elements identified as personal information by States are captured and listed. Awareness of this expanded list of personal information by multiple States will have value to industry participants.

A generalized use case demonstrates five data processing functional areas: collection, processing, transfer, storage, and disposal. Within each data process area, threats and vulnerabilities are listed. Recommendations are then proposed for policies, procedures, technologies, and incident response plans. Various MISMO process areas contributed to the drafting of the guidelines. As with State legislation, technology and practices are moving targets. The ISWG deferred to generally recognized standards organizations for specifications and recommendations. Leveraging well-known standards for the guidelines provides mortgage industry participants with credible practices that will help meet the requirements of auditors or compliance officers.

### **1.3 Purpose of Guidelines**

This guide is intended to assist the mortgage industry with privacy protection practices, and as such it provides guidance for developing and implementing preventive practices for your business. This guide does not provide a template that will guarantee compliance with state or federal regulatory requirements concerning the protection and handling of personal information.

Although state and federal laws impose enforceable requirements on businesses regarding personal information, the laws generally do not indicate what specific procedures or technologies companies must adopt in order to comply. We believe that by suggesting guidelines for the mortgage industry that are consistent with the previously articulated recommendations of recognized standards-setting organizations, this guide provides information helpful in establishing defensible information security policies and procedures for mortgage industry. This paper does not substitute for legal advice, and you should consult with qualified legal counsel regarding compliance requirements particular to your business.

Information security is a rapidly developing field. As the environment develops and matures, this document will be revised to accommodate changes in law, technology, and industry practices. Additionally, all parties must seek and monitor current and relevant information on personal privacy.

## **2. State Legislation**

### **2.1. CA SB 1386 Overview**

As the model framework for most unauthorized access notification laws an overview of CA SB 1386 is highlighted for generic content knowledge. The law is officially codified as California Civil Code sections 1798.29 and 1798.82 to 1798.84.

California was one of the first States to address personal privacy of consumer information. What distinguishes California's regulations from previous regulations is that the owner of the computerized (personal) information is liable for unauthorized disclosures of that information unless the owner acts promptly to notify all harmed parties. Historically, businesses such as mortgage lenders were able to pursue criminal litigation against offending parties when unauthorized acts of disclosure of personal information occurred. While this has not changed, California law now states that the mortgage lender is liable if corrective action and notification are not performed. Owners of personal information are no longer just a victim, but they assume responsibility and liability for the protection of that personal information.

CA SB 1386 requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California

whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.<sup>1</sup>

The law is intended to create better protection of personal information and to motivate faster response after unauthorized disclosure occurs.

- The law is intended to protect unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.<sup>2</sup>
- The law is intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crimes' impact.<sup>3</sup>

CA SB 1386 has three main provisions: identification of personal information, security breaches, and notification. Personal information is defined as unencrypted computerized data that contains the *combination* of an individual's name and one or more specific data elements. Specific data elements include social security number; driver's license or California Identification Card number; and financial account number with associated activation information. When unauthorized events occur, the owner of the information is required to notify all harmed parties.

Security breach is the unauthorized access, use, disclosure, or modification of electronic data. Owners of personal privacy information are obligated to protect against illegal or unofficial use of that information and are mandated to implement appropriate security safeguards.

A timely response (notification) to unauthorized disclosure is the third provision defined within CA SB 1386. The bill outlines whom to notify, when, and several options for how to provide notification. A "notice" may be provided in written notice, electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code, or a substitute notice. Substitute notices are used if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of E-mail notice when the agency has an e-mail address for the subject persons, conspicuous posting of the notice on the agency's Web site page, or notification to major statewide media.

## **2.2 CA SB 1386**

Three points of interest summarize the bill in relation to technology and business practices within the mortgage industry.

### **2.2.1 Personal Information**

CA SB 1386 is specific with respect to identifiable personal information:

*“an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:*

- (1) Social security number.*
- (2) Driver's license number or California Identification Card number.*

---

<sup>1</sup> CA SB 1386

<sup>2</sup> Recommended Practices on Notification of Security Breach Involving Personal Information

<sup>3</sup> Recommended Practices on Notification of Security Breach Involving Personal Information

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

*Personal information does not include:*

*“Any publicly available information that is lawfully made available to the general public from federal, state, or local government records.”*

## **2.2.2 Unauthorized Access**

Any breach of personal information as defined within CA SB 1386 or any reasonable belief that said data is acquired by an unauthorized person, needs to be disclosed through either a written or electronic notice to the affected resident of California.

## **2.2.3 Encryption Safe Harbor**

Through encryption of electronic data containing personal information an organization is compliant with CA SB 1386 even in the case of a breach. An organization has no legal obligation or liability under CA SB 1386 to disclose the breach publicly or notify the affected California resident.

## **2.3 Privacy Protection White Paper**

The California Office for Privacy Protection (COPP) developed *Recommended Practices on Notification of Security Breach Involving Personal Information*<sup>4</sup> to assist organizations in understanding and complying with CA SB 1386. That document provides the following information:

- Overview of CA SB 1386;
- Recommended practices for protecting the confidentiality of personal information, as well as implementing technologies (including encryption satisfying NIST standards) and procedures for preventing unauthorized access to that information;
- Recommended practices for organizational preparedness in the event a security breach occurs and notification under CA SB 1386 is required, as well as integration into an organization's security incident response program;
- Recommended practices for providing notification in accordance with CA SB 1386 upon a security breach occurring;
- Sample notices for use to comply with CA SB 1386;
- The text from CA SB 1386;
- Information on reporting computer crimes to law enforcement;
- Pointers to information security resources;
- Benchmark results on how some companies have reacted to CA SB 1386.

Although the recommendations in the COPP white paper are not legally binding, the COPP is a government agency charged by statute with making recommendations to organizations concerning privacy policies and practices. The MISMO ISWG recommends that institutions within the mortgage industry embrace the recommended practices developed by COPP, and specifically incorporate the COPP's recommendations into organizational security incident

---

<sup>4</sup> The recommended practices can be downloaded from <http://www.privacy.ca.gov/recommendations/secbreach.pdf>.

response programs. These recommended practices go beyond notification of security breaches relating to California residents, and can apply to any security breach associated with the unauthorized disclosure of personal information.

## **2.4 Other States Legislation**

### **2.4.1 Introduction**

The following treatise has been created by the MISMO Information Security Workgroup (ISWG) to review some of the general aspects related to Personal Information (PI) protection and more specifically to discuss which MISMO defined data points (i.e., data elements) fall into the general category of defined PI when addressing the organizational controls that would need to be considered for developing a response to the security breach notification aspects of these various state laws.

Section 4 of this document lists several references from which the ISWG gathered information about PI and notification legislation. In reviewing the information from the referenced sites it is important to understand that PI data points can be defined in a multitude of ways dependent on the context in which PI is being discussed. Some states have separate legislation for criminal and non-criminal activity security breach notification, while other states combine everything into a single piece of legislation. When combined legislation is presented, it is not uncommon to find a definition of personal information data elements under the law enforcement section and then personal information being redefined in a notification section. If the legislation is separate the same piece of data can be defined very differently from one act to another within the same State. This often leads to confusion with respect to identification of data elements specific to notification. In addition, bills can contain language that concern law enforcement behavior, security freeze requirements, credit reports, disposal, or recording requirements. It is important for businesses to take care when performing their due diligence with notification

Personal information and notification law is a dynamic environment. The number of states that have passed or have pending legislation in development or review will change from month-to-month or even week-to-week. It is important to not dwell on numbers such as “18 states”, but rather the general context of the information.

As of November, 2005 18 states have passed legislation requiring notification if personal information has been compromised (or "breached"), and more than a dozen other states have drafts pending. The expectation is for these numbers to increase over the coming months. Additionally, there are a number of federal proposals on this same subject being vetted in the U.S. Senate and House of Representatives. Relief at the federal level appears to be at least a year away. If you apply the 80/20 rule to this legislative activity, 80% of the state bills mirror CA SB 1386 with respect to personal information. Unfortunately, the 20% of states that have expanded the definition of PI, notification triggers, media, and safe harbor are the ones that present difficult challenges for the mortgage industry. There is also a need to consider Gramm-Leach-Bliley (GLB) applicability, so that State legislation effectively builds on and/or leverages GLB privacy stipulations.

### **2.4.2 Idiosyncrasies of Bills**

Most of the bills are for “computerized” information where the confidentiality and integrity of PI are compromised by unauthorized individuals. The term computerized is a critical definition that allows policies to be written under a defined scope. However, several State bills, such as Alaska (proposed) and North Carolina address all media, which would include paper, facsimile, or other

physical media. At the Federal level the “*Notification of Risk to Personal Data Act*,” S.751 which was introduced on April 11, 2005 by Senator Feinstein (CA) addresses all media types. If passed as stated, the result of this legislation could have a large impact on existing operations, both technically and procedurally. The scope of this paper is concerned primarily with computerized data practices, although it is worth noting that organizations will need to address more than their electronic based records as a result of this legislation.

Encryption is generally specified as a safe harbor for PI. But, there are a few States that don’t provide a specific reference or exclusion for encryption. Some of the proposed state bills do not explicitly state “not encrypted” for personal information data elements. There appears to be two possible conclusions. One, all security breaches are to be reported whether data is encrypted or not. Two, businesses are to assess whether the confidentiality or integrity of the data present a security breach. Option two may lead to the subjective interpretation of a breach and therefore the potential of some breaches not being reported. This question can not be answered within the context of this document. The best recommendation would be to review any relative case law and consult your legal counsel concerning the handling of data that may be subject to state laws that do not provide an explicit encryption exemption.

The common thread on data points within the various laws being proposed or having passed is that data points alone are not at issue, but rather it is a combination of data that is cause for concern. A consumer name in combination with a social security number, driver’s license number, and/or state identification card number, and financial account numbers, credit or debit card numbers along with associated access codes (pins/passwords), trigger notification. Strict interpretation of the bills indicates that a list of social security numbers, in and of themselves, if compromised, does not require notice. Names in combination with account number if compromised may not require notice, if there is a separate PIN or password required to access the account. Driver’s licenses and financial account information if compromised typically do not require notice. However, the general trend with security breaches is to make public such events whether they meet the letter of the law or not. When and to what extent security breaches are made public or disclosed is the responsibility of the organization.

As outlined in the previous paragraph and in general credit and debit card numbers may only require notification when combined with access codes, PINs, or passwords if required to access an account. However this condition is not true for all states. New York does not qualify access codes, PINS, or passwords for a breach of account, credit, and debit numbers. This is another example of the inconsistency of the State notification bills. A recommended practice is for businesses to evaluate action concerning financial accounts regardless of any compromise of access codes, PINs, or passwords.

Another difficulty with respect to data elements classified as sensitive is the expanded list of items identified by some states: Date of Birth (DoB), Address, Phone Number, Mother’s Maiden Name, Passport Number, Automated or Electronic Signatures, Biometric Data, Fingerprints, Medical Information, Employment Information, Employment History, Financial Device, and Education. The legislation does not define these sensitive data elements nor provide guidance with interpretation. The ability for an organization to establish a common policy governing this extensive list of items is problematic. Customer email addresses and account numbers are used as search criteria or database keys in many instances. Restricting access or encrypting these fields would lead to major redesigns of existing applications.

The legislation generally states the “owner” of the PI is responsible for notification and other actions, as well as financial costs. The nature of any mortgage transaction is the connection of

multiple business partners required to complete the funding of a loan. Personal information is collected by loan originators, while information brokers maintain repositories on personal assets, liabilities and payment history. As mortgage promissory notes migrate through their life cycle from the primary origination market to the secondary investor market and are used to create mortgage backed securities, identifying ownership of personal information is difficult to pinpoint and track. A direct line of ownership of the personal information is not always clear. Liabilities associated with the ownership and responsibility of security breach notifications are not well defined within the legislation.

The legislation contains rules governing procedures for notification. The timing of notification is in the most expedient time possible and without unreasonable delay. Exceptions are provided when requested by law enforcement. Methods for notification include written, electronic, public media, websites, etc. When and which method to be used are often governed by each state's specific bill. These granular notification procedures and triggers will be a major obstacle to implementation or the ability to provide generic guidelines.

Questions to consider include how to implement a general security program when there are differing legal requirements from a minority of states. Do organizations create a security policy based on a majority of the laws and then implement exception procedures for the expanded laws or a single policy based on the least common set of requirements across all law? What is the cost of implementing an expanded policy for all state legislation versus the risk of securing only a minimum set of data elements with exception procedures? Again, these are questions best addressed with legal counsel in light of the particular circumstances of your business.

### **2.4.3 Personal Information Identified in State Legislation**

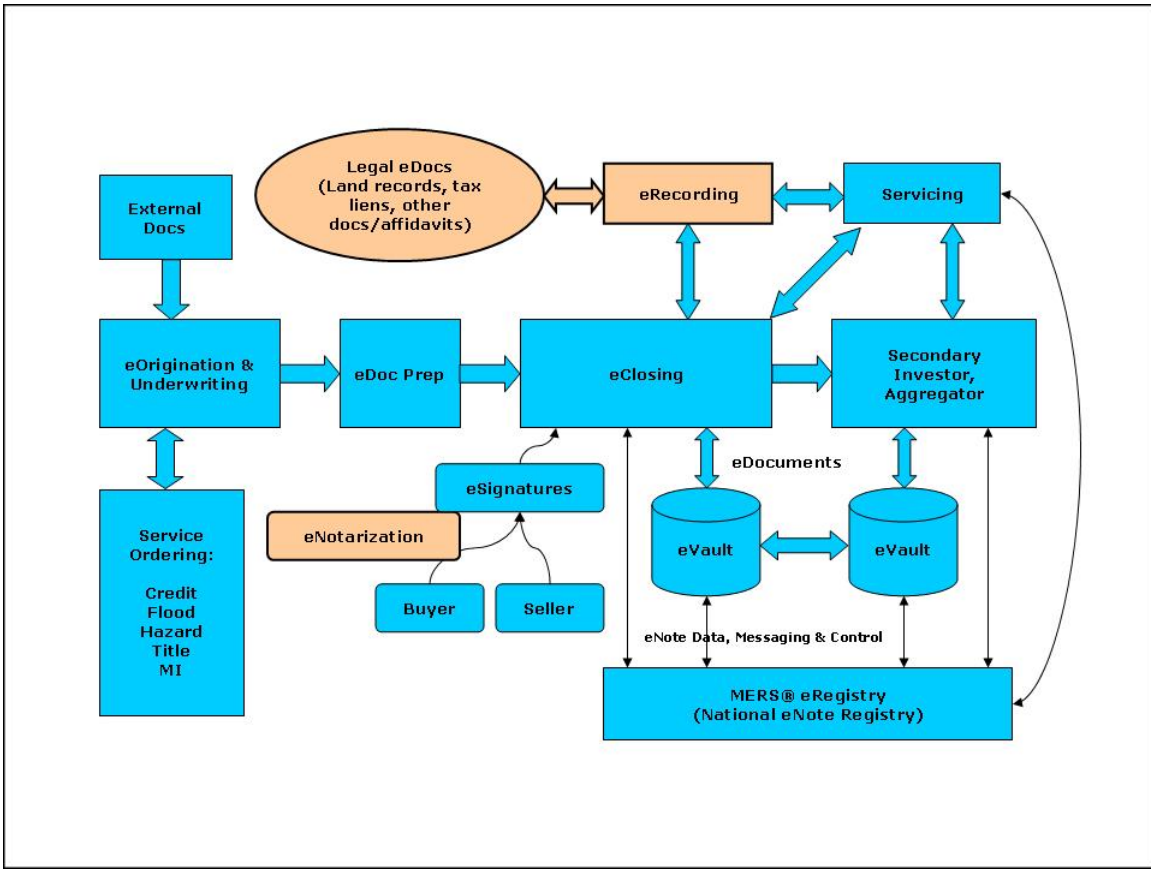
1. Individual's first name or first initial and last name
2. Social security number (SSN)
3. Driver's License Number or Personal and/or State ID Number
4. Any Financial Account Number (checking accounts, saving accounts, credit card, debit card, pin/password)
5. Individual's date of birth (DOB)
6. Maiden name of the individual's mother or Parent's surname.
7. Automated Electronic, or Digital Signatures
8. Individual's digitized or other electronic signature
9. "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional
10. Identification number assigned to the individual by the individual's employer

## **3. Guidelines for Safeguarding Personal Information**

In addition to the recommended practices developed by the California Office for Privacy Protection (COPP),<sup>5</sup> the following recommendations are provided that specifically relate to the mortgage industry and electronic mortgages. The general electronic mortgage process flow is depicted in Figure 1.

---

<sup>5</sup> <http://www.privacy.ca.gov/recommendations/secbreach.pdf>



**Figure 1: Electronic Mortgage Flow Diagram**

Throughout the flows of the electronic mortgage process, as depicted in Figure 1, there are many points where personal information is *collected, processed, transferred, stored* and eventually *disposed*. Each of these critical areas in handling personal information presents different issues that need to be addressed and resolved by mortgage industry institutions to ensure that personal information is being protected adequately and in accordance with applicable legislations. Within each of these areas, organizations need to understand the applicable threats and vulnerabilities that can lead to the unauthorized disclosure of personal information in human readable form; the policies, procedures and technologies that can be implemented to protect against the unauthorized disclosure of personal information; and in the event an unauthorized disclosure does occur, the incident response plans that an organization can follow to mitigate the overall risk for disclosing the personal information.

For the purposes of this paper, the following definitions are used for threats, vulnerabilities and risks:

*Threat* – Something that is the source for causing danger or harm. For example, a hacker is a threat to a company’s computer system.

*Vulnerability* – Something that is susceptible to attack or harm. For example, an un-patched computer system is vulnerable to an attack by an Internet virus.

*Risk* – The undesired result (consequence) that occurs when a threat successfully attacks or exploits vulnerability. For example, an Internet virus (*threat*) penetrates an un-patched computer system (*vulnerability*) and causes the computer system to disclose personal information in an unauthorized manner (*risk*). Risk is further defined as having two components: the likelihood that the consequence will occur, and the severity of the consequence.

The remainder of this section provides an analysis for each of the five critical areas with respect to threats and vulnerabilities; policies, procedures and technologies; and incident response plans. The analysis is based on a general, web-based, consumer-to-business use case (see Figure 2) that is applicable to many electronic mortgage environments, as well as physical environments. In addition, the analysis focuses in on PI specifically, recognizing that PI exists in many different mortgage documents and that it would be difficult to address PI within the context of each of these documents. [Note: The recommendations provided in this paper can also be applied to protecting sensitive information of employees and business partners.]

The MISMO ISWG also highly recommends that mortgage industry institutions implement programs that educate employees on the importance of protecting personal information, and the important role that each employee has in performing his/her duties to ensure that personal information is *collected, processed, transferred, stored* and *disposed* in a secure manner.

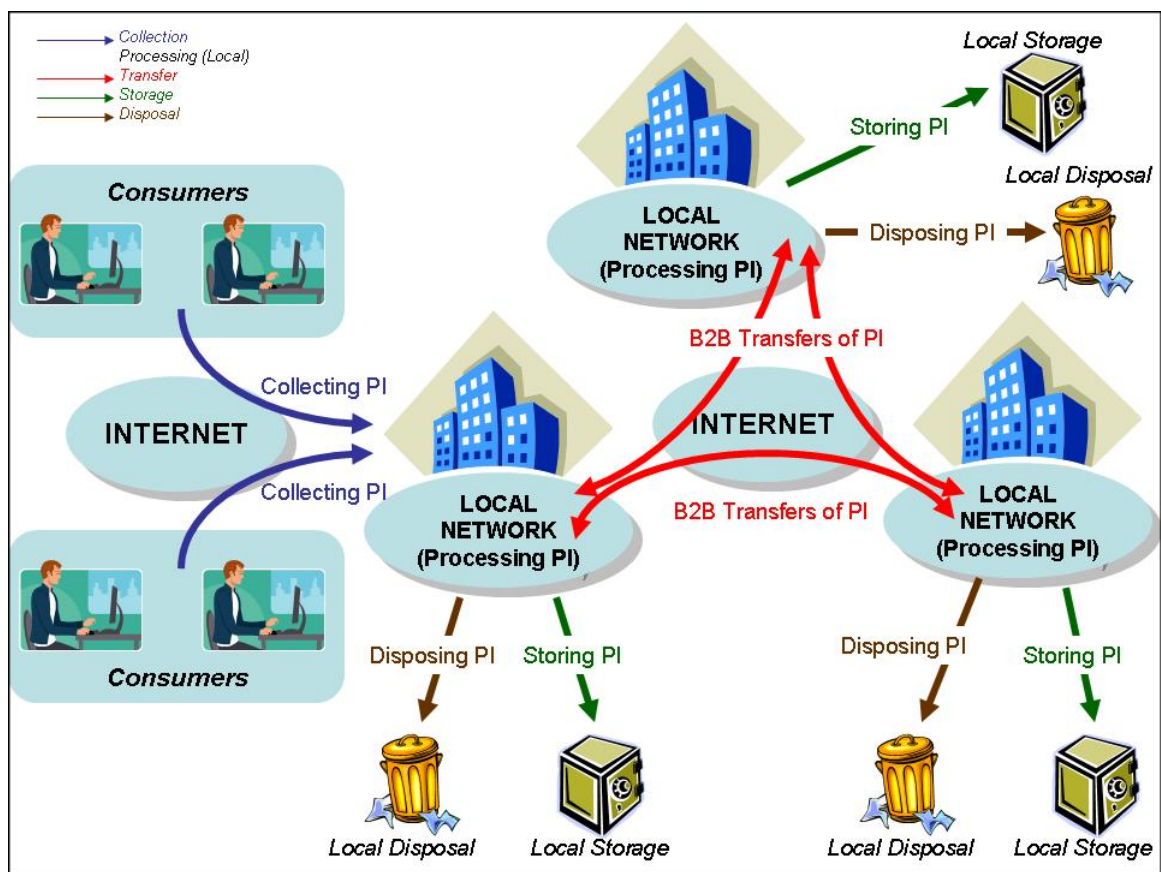


Figure 2: General PI Use Case

### 3.1. Analysis of PI Use Cases – Threats, Vulnerabilities & Risks

This section analyzes each PI use case and identifies threats, vulnerabilities, and resulting risks that are specific to each PI use case.

#### 3.1.1 Collection of Personal Information

##### 3.1.1.1. Definition

*Collection* – Collection of PI is the initial gathering of personal information from a consumer to support an electronic mortgage function or process. In other words, a consumer (e.g. applicant, borrower) is **personally responsible** for submitting his/her personal information to a mortgage institution/entity for the purpose of fulfilling some electronic mortgage function (e.g., submission of a loan application, customer support function).

In Figure 2 *collection* of PI is assumed as coming directly from a consumer to a mortgage entity. If a mortgage entity receives PI from another company or a representative of the consumer, this is considered *B2B transferring* of PI for the purpose of this paper, which is addressed in section 3.1.3. The reason for this distinction is due to the point of view that this paper takes, which is the point of view from the consumer. From the consumer's point of view, PI is *collected* when the consumer personally provides it. From that point on (and again from the consumer's viewpoint), the data is *processed, transferred, stored* and eventually *disposed*.

##### 3.1.1.2. Threats and Vulnerabilities

Figure 3 represents a general use case where PI is being collected from a consumer through a web based interface at a mortgage entity (e.g., filling out a loan application). Within this use case, common threats and vulnerabilities are highlighted.

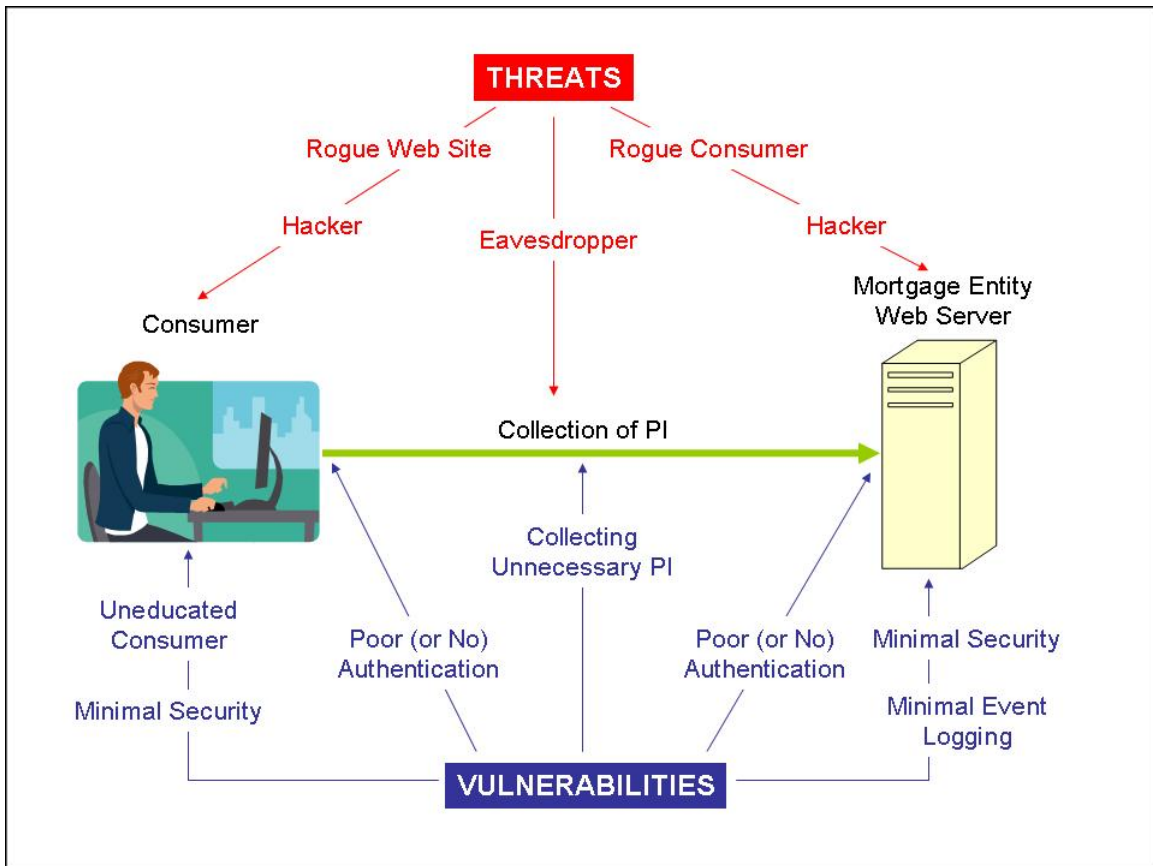


Figure 3: PI Collection Use Case

Threats:

- *Rogue Consumer* – An entity posing to be a legitimate consumer.
- *Hacker* – An entity purposely attempting to gain unauthorized access to computer systems.
- *Eavesdropper* – An entity that is capable of intercepting PI (without knowledge by the consumer or the mortgage entity) as it is collected by the mortgage entity from the consumer.
- *Rogue Web Site* – A web site that poses to be a legitimate web site (i.e., a real on-line mortgage entity) for the purposes of collecting PI (e.g., phishing, pharming).

Vulnerabilities:

- *Collecting Unnecessary PI* – A mortgage entity that collects PI that is not needed to support electronic mortgage functions or processes.
- *Poor Authentication* – An inability for either the consumer or the mortgage entity to authenticate one another prior to executing on-line transactions.
- *Minimal Security (Mortgage Entity Web Interface)* – Minimal or poor security at the web interface (e.g., web server) that leads to exposure of PI as it is being collected by the consumer. Specific vulnerabilities include:
  - Use of non-secure protocols (e.g., http vs. https)
  - No use of firewalls or poor configuration of firewalls
  - Out of date security patches on web server
  - Unneeded cached PI data resident on web server
  - Lack of intrusion detection / intrusion prevention capabilities

- Poor key management to support cryptographic functions (e.g., SSL)
- Insecure configuration of web server, including lack of audit to verify configuration
- Out of date virus detection capabilities
- *Minimal Security (Consumer Computer)* – Minimal or poor security at the consumer’s computer that leads to exposure of the consumer’s PI. Specific vulnerabilities include:
  - Lack of firewall capabilities
  - Out of date security patches
  - Out of date virus protection capabilities
  - Cached PI data
- *Minimal Event Logging* – Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
- *Uneducated Consumer* – A consumer who has little to no security knowledge with respect to participating in on-line transactions. These consumers don’t understand the importance of implementing security controls on their own computers, nor are they able to distinguish the difference between a good web site vs. a rogue web site.

Table 1 provides a mapping of threats to vulnerabilities, and also defines the resultant risk for when threats exploit vulnerabilities while PI is being collected.

**Table 1: Collecting PI Threats and Vulnerabilities**

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
Rogue Consumer	Poor Authentication	Mortgage entity may divulge PI to a person who is posing as a legitimate consumer.
	Minimal Event Logging	Mortgage entity is unaware of masquerader’s tactics in collecting PI.
Hacker	Collecting Unnecessary PI	Hacker gains access to additional PI that is not even needed by mortgage entity.
	Poor Authentication	Hacker gains access to computing systems (consumer and mortgage entity) containing PI.
	Minimal Security (Mortgage Entity)	Hacker gains access to mortgage entity networks and computing systems containing PI.
	Minimal Security (Consumer)	Hacker gains access to consumer computing environment containing PI (e.g., cached data).
	Minimal Event Logging	Hacker’s activities in collecting PI go unnoticed by mortgage entity.
Eavesdropper	Minimal Security	Eavesdropper is capable of intercepting PI that is poorly protected, or not protected at all (e.g., weak cryptography, insecure protocols).
	Collecting Unnecessary PI	Eavesdropper gains more PI than originally anticipated.
Rogue Web Site	Poor Authentication	Consumer not able to properly authenticate to determine if web site is valid or rogue.
	Minimal Security (Consumer)	Rogue web site able to download malicious software capable of collecting PI.
	Uneducated Consumer	Rogue web site able to socially engineer consumer into thinking web site is valid for purpose of collecting PI (e.g., phishing, pharming).

## 3.1.2. Processing of Personal Information

### 3.1.2.1. Definition

*Processing* – Processing of PI is an organization’s internal use of personal information, by their employee(s) or computing environment, to execute an electronic mortgage workflow activity (e.g., loan processing). *Processing* includes electronic computer processing as well as human review of electronic personal information.

In Figure 2 *processing* is assumed to be performed within the boundaries of a mortgage entity, and within a local operational network.<sup>6</sup> If a high level function (e.g., document preparation) involves multiple mortgage entities working together to *process* PI, a *B2B transfer* of PI is required to *transfer* PI to each mortgage entity. It is important to note this distinction between internal *processing* and *B2B transfers* because it helps a mortgage entity define boundaries for when PI exists within the mortgage entity, and when it does not, for the purpose of fulfilling an electronic mortgage function.

### 3.1.2.2. Threats and Vulnerabilities

Figure 4 represents a general use case where PI is being processed within a mortgage entity (e.g., processing a loan application). Within this use case, common threats and vulnerabilities are highlighted.

---

<sup>6</sup> Local operational network is a notional term. A mortgage entity needs to determine within its own working boundaries what constitutes a local operational network (e.g., LAN, WAN) where *processing* occurs, vs. *transferring* PI to other operational networks (either internally within the organization or to other mortgage entities).

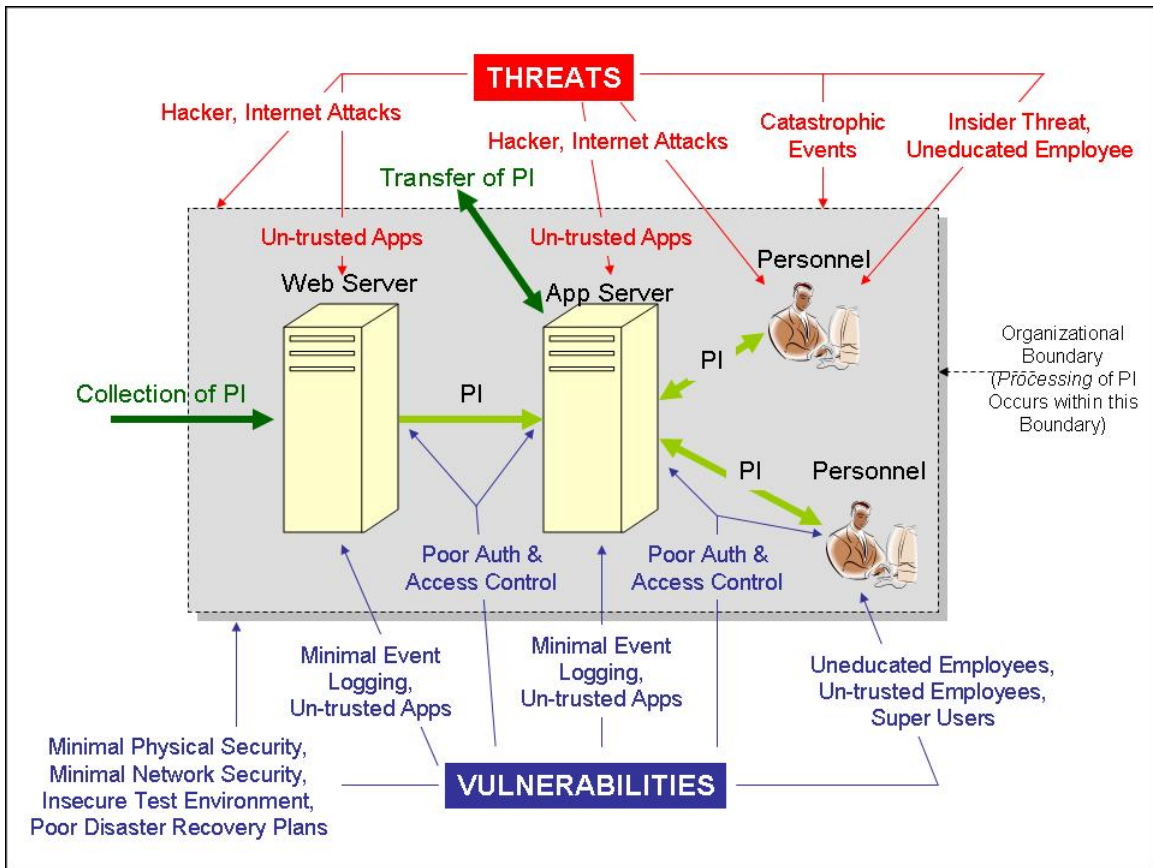


Figure 4: Processing of PI within a Mortgage Entity

Threats:

- *Hacker* – An entity purposely attempting to gain unauthorized access to computer systems.
- *Internet-based Attack* – Worms, viruses, etc., that promulgate via the Internet and look to exploit vulnerabilities within computing networks and systems.
- *Insider Threat* – An employee, contractor, etc., that has internal access to organizational assets, and intends to leverage that access to perform unauthorized functions.
- *Uneducated Employee* – An employee (or contractor) who unknowingly performs unauthorized functions (e.g., emailing PI over unprotected networks, screen prints of PI), is susceptible to social engineering attacks that disclose PI, or performs ill-advised functions due to lack of education (e.g., poor development and testing practices, inappropriate use of PI in testing environments).
- *Un-trusted Applications* – Applications that perform functions they are not supposed to perform, or do not perform functions they are supposed to perform.
- *Catastrophic Events* – Unforeseen events (e.g., natural disasters, major power outages) that cause operations to cease.

Vulnerabilities:

- *Poor Authentication & Access Control* – An inability to authenticate individuals and applications involved in processing PI, as well as determining the privileges & authorizations of individuals and applications.
- *Minimal Network Security* – Minimal or poor enterprise network security that leads to exposure of PI as it is being processed. Specific vulnerabilities include:

- Use of non-secure protocols (e.g., SQL, RPC, unprotected email)
- No use of firewalls or poor configuration of firewalls
- Out of date security patches on computing equipment
- Unneeded cached PI data resident on computing equipment
- Lack of intrusion detection / intrusion prevention capabilities
- Poor key management to support cryptographic functions (e.g., SSH)
- Insecure configuration of computing equipment, including lack of audit to verify configuration
- Out of date virus detection capabilities
- *Minimal Physical Security* – Minimal or poor physical security to prevent unauthorized access to critical computing equipment.
- *Minimal Event Logging* – Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
- *Uneducated Employee* – An employee (or contractor) who has little to no security awareness as it relates to the performance of his/her job, and specifically to the handling of PI.
- *Un-trusted Employee* – An employee (or contractor) performing in a trusted role (e.g., database administrator with access to PI) without having the necessary qualifications fulfilled for that trusted role (e.g., background check).
- *Super User* – An employee (or contractor) with too many privileges, most of which are not needed for the employee (contractor) to perform his/her functions.
- *Un-trusted Applications* – Sensitive applications (i.e., that process PI) that do not meet specific security and trust requirements. Un-trusted applications may be due to:
  - Poor requirements specification
  - Poor development and coding practices
  - Poor testing practices
  - Complexity within the application
- *Insecure Test Environment* – Test environments that use “live operational data” but have lax security capabilities compared to the operational environments.
- *Poor Disaster Recovery Plans and Capabilities* – Plans and capabilities that do not exist, or exist but are in such poor condition that an organization is unable to recover back to adequate operating state after a catastrophic event has occurred.

Table 2 provides a mapping of threats to vulnerabilities, and also defines the resultant risk for when threats exploit vulnerabilities while PI is being processed.

**Table 2: Processing PI Threats and Vulnerabilities**

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
Hacker	Poor Authentication & Access Control	Hacker gains access to PI that is resident on internal computing systems.
	Minimal Network Security	Hacker gains access to mortgage entity networks and computing systems containing PI.
	Minimal Event Logging	Hacker’s activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Hacker is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Hacker corroborates with un-trusted employee in gaining access to systems containing PI.
	Super User	Hacker corroborates with an employee that has

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
		privileges to gain access into systems containing PI.
	Un-trusted Applications	Hacker is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications in obtaining PI.
	Insecure Test Environment	Hacker gains access to PI that is resident in the test environment.
Internet-based Attack	Minimal Network Security	Worm, virus, etc., is capable of penetrating enterprise network and computing systems and causing applications to disclose PI.
	Minimal Event Logging	Internet attack goes unnoticed by mortgage entity, or is noticed after PI has been disclosed.
	Uneducated Employee	Employee is socially engineered (e.g., phishing) into launching an Internet attack within the enterprise with the intent to disclose PI.
	Un-trusted Application	Internet attack leverages a known vulnerability (i.e., an un-trusted process) in a product or application to disclose PI.
	Insecure Test Environment	Worm, virus, etc., is capable of penetrating test environment causing the disclosure of PI.
Insider Threat	Minimal Network Security	Insider gains easy network access to mortgage entity networks and computing systems containing PI.
	Minimal Physical Security	Insider gains easy physical access to mortgage entity networks and computing systems containing PI.
	Minimal Event Logging	Insider's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Insider is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Insider corroborates with un-trusted employee in gaining access to systems containing PI.
	Super User	Insider corroborates with an employee that has privileges to gain access into systems containing PI.
	Un-trusted Applications	Insider is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications in obtaining PI.
	Insecure Test Environment	Insider gains access to PI that is resident in the test environment.
Uneducated Employee	Uneducated Employee	An employee with little to no security awareness or training is a threat waiting to exploit its own vulnerability. These employees typically do not understand the importance for protecting PI, and in basic terms "don't know what they don't know." They perform activities that typically

Threat	Vulnerability	Risk
		involve providing PI to anyone who claims a need to have it.
	Minimal Event Logging	Uneducated employee's (accidental) activities in disclosing PI go unnoticed by mortgage entity.
Un-trusted Applications	Un-trusted Applications	Similar to uneducated employees, un-trusted applications can be a threat waiting to exploit their own vulnerabilities. Due to lack of testing, poor development practices, etc., these applications perform functions that are not supposed to be performed, and vice-versa, which can lead to disclosure of PI.
	Minimal Event Logging	Un-trusted application's (unanticipated) activities in disclosing PI go unnoticed by mortgage entity.
Catastrophic Event	Poor Disaster Recovery Plans and Capabilities	If disaster recovery and business continuity plans and capabilities do not provide for an operational environment that is as secure as the original operating environment, then all the above threats, vulnerabilities and exploitations apply to the environment operating in disaster recovery mode.

### 3.1.3. B2B Transferring of Personal Information

#### 3.1.3.1. Definition

*Transferring* – Transferring of PI is the sending and receiving of personal information between two mortgage entities.

In Figure 2 *transferring* is assumed to be performed after PI has been initially *collected* from the consumer, and in support of *processing* and *storing* PI. That is, *transferring* of PI is not considered a stand-alone function. It is performed as part of a general *processing* or *storing* function. *Disposing* of PI is considered to be a local matter within a mortgage entity; therefore, it is not necessary to *transfer* PI to another entity for the purpose of *disposing* the PI.

#### 3.1.3.2. Threats and Vulnerabilities

Figure 5 represents a general use case where PI is being transferred between mortgage entities (e.g., corroborating applicant information to support loan approval functions). Within this use case, common threats and vulnerabilities are highlighted.

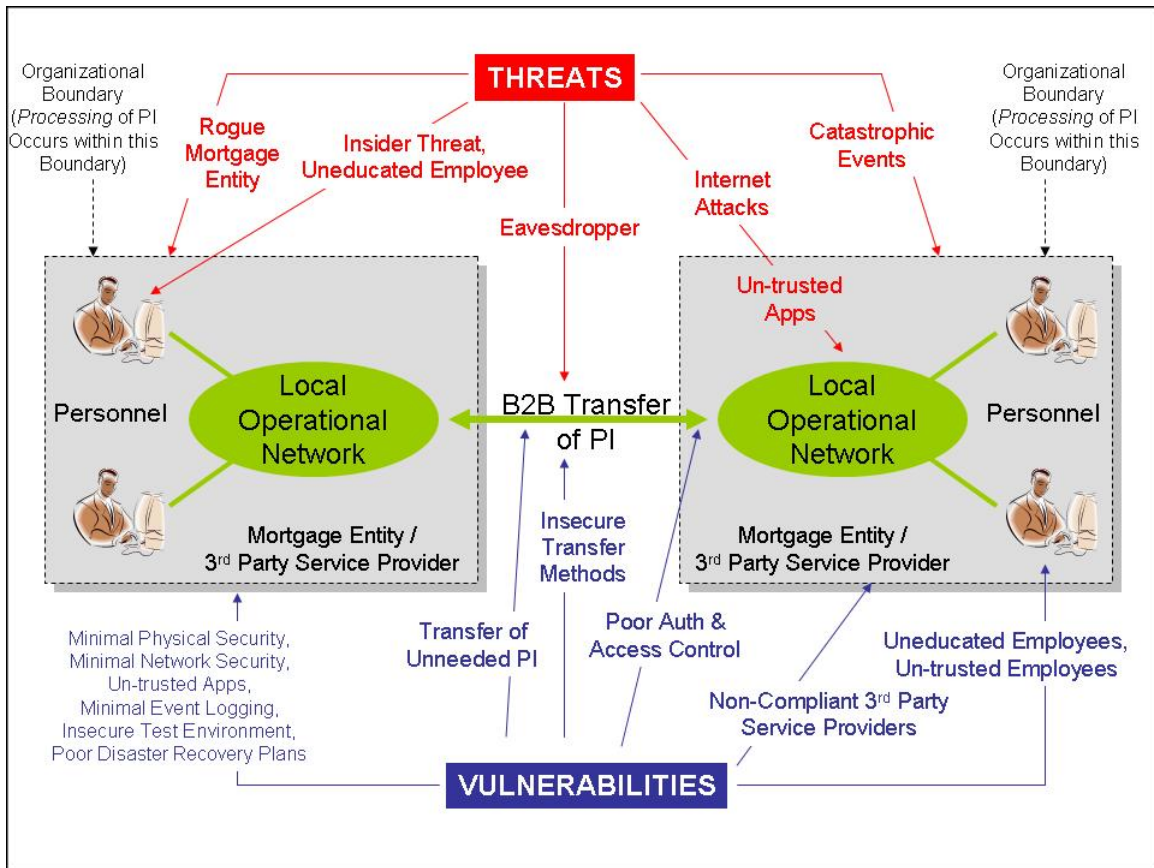


Figure 5: Transferring of PI Between Two Mortgage Entities

Threats:

- *Rogue Mortgage Entity* – An entity that poses to be a legitimate mortgage entity for the purposes of collecting PI.
- *Insider Threat* – An employee, contractor, etc., that has internal access to organizational assets, and intends to leverage that access to perform unauthorized functions.
- *Uneducated Employee* – An employee (or contractor) who unknowingly performs unauthorized functions (e.g., emailing PI over unprotected networks, screen prints of PI), is susceptible to social engineering attacks that disclose PI, or performs ill-advised functions due to lack of education (e.g., poor development and testing practices, inappropriate use of PI in testing environments).
- *Eavesdropper* – An entity that is capable of intercepting PI (without knowledge by either mortgage entity) as it is transferred between mortgage entities.
- *Internet-based Attack* – Worms, viruses, etc., that promulgate via the Internet and look to exploit vulnerabilities within computing networks and systems.
- *Un-trusted Applications* – Applications that perform functions they are not supposed to perform, or do not perform functions they are supposed to perform.
- *Catastrophic Events* – Unforeseen events (e.g., natural disasters, major power outages) that cause operations to cease.

Vulnerabilities:

- *Minimal Physical Security* – Minimal or poor physical security to prevent unauthorized access to critical computing equipment.

- *Minimal Network Security* – Minimal or poor enterprise network security that leads to exposure of PI as it is being transferred. Specific vulnerabilities include:
  - Use of non-secure protocols (e.g., FTP, HTTP, unprotected email)
  - No use of firewalls or poor configuration of firewalls
  - Out of date security patches on computing equipment
  - Unneeded cached PI data resident on computing equipment
  - Lack of intrusion detection / intrusion prevention capabilities
  - Poor key management to support cryptographic functions (e.g., SSL)
  - Insecure configuration of computing equipment, including lack of audit to verify configuration
  - Out of date virus detection capabilities
- *Minimal Event Logging* – Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
- *Insecure Test Environment* – Test environments that use “live operational data” but have lax security capabilities compared to the operational environments.
- *Poor Disaster Recovery Plans and Capabilities* – Plans and capabilities that do not exist, or exist but are in such poor condition that an organization is unable to recover back to adequate operating state after a catastrophic event has occurred.
- *Transferring Unnecessary PI* – A mortgage entity that transfers additional PI that is not needed by the recipient mortgage entity.
- *Insecure Transfer Methods* – Electronic (e.g., Internet-based) and physical (e.g., media) transfer methods that do not provide adequate protection of PI (e.g., PI is not encrypted while in transit).
- *Poor Authentication & Access Control* – An inability to authenticate individuals and applications involved in transferring PI, as well as determining the privileges & authorizations of individuals and applications.
- *Non-Compliant 3<sup>rd</sup> Party Service Providers* – Mortgage entities that do not perform periodic security reviews or audits to understand the security posture of their organization.
- *Uneducated Employee* – An employee (or contractor) who has little to no security awareness as it relates to the performance of his/her job, and specifically to the handling of PI.
- *Un-trusted Employee* – An employee (or contractor) performing in a trusted role (e.g., database administrator with access to PI) without having the necessary qualifications fulfilled for that trusted role (e.g., background check).
- *Un-trusted Applications* – Sensitive applications (i.e., that process PI) that do not meet specific security and trust requirements. Un-trusted applications may be due to:
  - Poor requirements specification
  - Poor development and coding practices
  - Poor testing practices
  - Complexity within the application

Table 3 provides a mapping of threats to vulnerabilities, and also defines the resultant risk for when threats exploit vulnerabilities while PI is being transferred.

**Table 3: Transferring PI Threats and Vulnerabilities**

Threat	Vulnerability	Risk
Rogue Mortgage Entity	Poor Authentication & Access Control	Rogue entity gains access to PI that is being transferred to the rogue entity.
	Insecure Transfer	Rogue entity requires trivial effort and resources

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
	Methods	to extract PI from transfer mechanisms (e.g., data is not encrypted).
	Transferring Unnecessary PI	Rogue entity gains more PI than originally anticipated.
	Minimal Event Logging	Rogue entity's actions go unnoticed by the valid mortgage entity transferring PI to the rogue entity.
	Uneducated Employee	Rogue entity is able to socially engineer an employee into disclosing PI.
	Un-trusted Employee	Rogue entity corroborates with un-trusted employee in obtaining transferred PI to the rogue entity.
	Non-compliant 3 <sup>rd</sup> Party Service Provider	Rogue entity leverages 3 <sup>rd</sup> party's lack of security awareness and general insecure environment to obtain transferred PI from 3 <sup>rd</sup> party.
Internet-based Attack	Minimal Network Security	Worm, virus, etc., is capable of penetrating enterprise network and computing systems and causing applications to disclose PI.
	Minimal Event Logging	Internet attack goes unnoticed by mortgage entity, or is noticed after PI has been disclosed.
	Uneducated Employee	Employee is socially engineered (e.g., phishing) into launching an Internet attack within the enterprise with the intent to disclose PI.
	Un-trusted Application	Internet attack leverages a known vulnerability (i.e., an un-trusted process) in a product or application to disclose PI.
	Non-compliant 3 <sup>rd</sup> Party Service Providers	3 <sup>rd</sup> party is ill-equipped to deal with Internet-based attacks, which can lead to the exposure of PI.
	Insecure Test Environment	Worm, virus, etc., is capable of penetrating test environment causing the disclosure of PI.
Insider Threat	Minimal Network Security	Insider gains easy network access to mortgage entity networks and computing systems containing PI.
	Minimal Physical Security	Insider gains easy physical access to mortgage entity networks and computing systems containing PI.
	Minimal Event Logging	Insider's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Insider is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Insider corroborates with un-trusted employee in gaining access to systems containing PI.
	Insecure Test Environment	Insider gains access to PI that is resident in the test environment.
	Un-trusted Applications	Insider is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications

Threat	Vulnerability	Risk
		in obtaining PI.
	Insecure Transfer Methods	Insider has an ability to easily transfer PI outside of an organization using unprotected channels (e.g., unprotected email, FTP).
Uneducated Employee	Uneducated Employee	An employee with little to no security awareness or training is a threat waiting to exploit its own vulnerability. These employees typically do not understand the importance for protecting PI, and in basic terms “don’t know what they don’t know.” They perform activities that typically involve providing PI to anyone who claims a need to have it.
	Minimal Event Logging	Uneducated employee’s (accidental) activities in disclosing PI go unnoticed by mortgage entity.
	Insecure Transfer Methods	Uneducated employee may not be aware that certain communication channels are unprotected, and may inadvertently distribute PI over those unprotected channels (e.g., unprotected email, FTP, HTTP).
Un-trusted Applications	Un-trusted Applications	Similar to uneducated employees, un-trusted applications can be a threat waiting to exploit their own vulnerabilities. Due to lack of testing, poor development practices, etc., these applications perform functions that are not supposed to be performed, and vice-versa, which can lead to disclosure of PI.
	Minimal Event Logging	Un-trusted application’s (unanticipated) activities in disclosing PI go unnoticed by mortgage entity.
Catastrophic Event	Poor Disaster Recovery Plans and Capabilities	If disaster recovery and business continuity plans and capabilities do not provide for an operational environment that is as secure as the original operating environment, then all the above threats, vulnerabilities and exploitations apply to the environment operating in disaster recovery mode.
Eavesdropper	Insecure Transfer Methods	Eavesdropper is capable of intercepting PI that is poorly protected, or not protected at all (e.g., weak cryptography, insecure protocols) while it is being transferred.
	Transferring Unnecessary PI	Eavesdropper gains more PI than originally anticipated.

### 3.1.4. Storing Personal Information

#### 3.1.4.1. Definition

*Storing* – Storing of PI is the placement of personal information into either temporary or long term containers. Temporary containers (e.g., workflow applications) are used to support real-time execution of an electronic mortgage process or function. Long term containers (e.g., eVault) are used to support historical record keeping and maintenance of electronic mortgage transactions.

In Figure 2, *storing* PI is assumed to occur after some local *processing* of PI is complete. For example, PI can be *stored* temporarily as part of *processing* a loan application from a consumer, *stored* long term in a local environment as part of closing a loan for a consumer, and *stored* long term in a remote environment as part of servicing the loan for a consumer (e.g., eVault). Note in this last example that the PI is *transferred* to the remote entity, *processed* by that remote entity, and then *stored* by that remote entity.

### 3.1.4.2. Threats and Vulnerabilities

Figure 6 represents a general use case where PI is being stored, locally as well as remotely. Within this use case, common threats and vulnerabilities are highlighted.

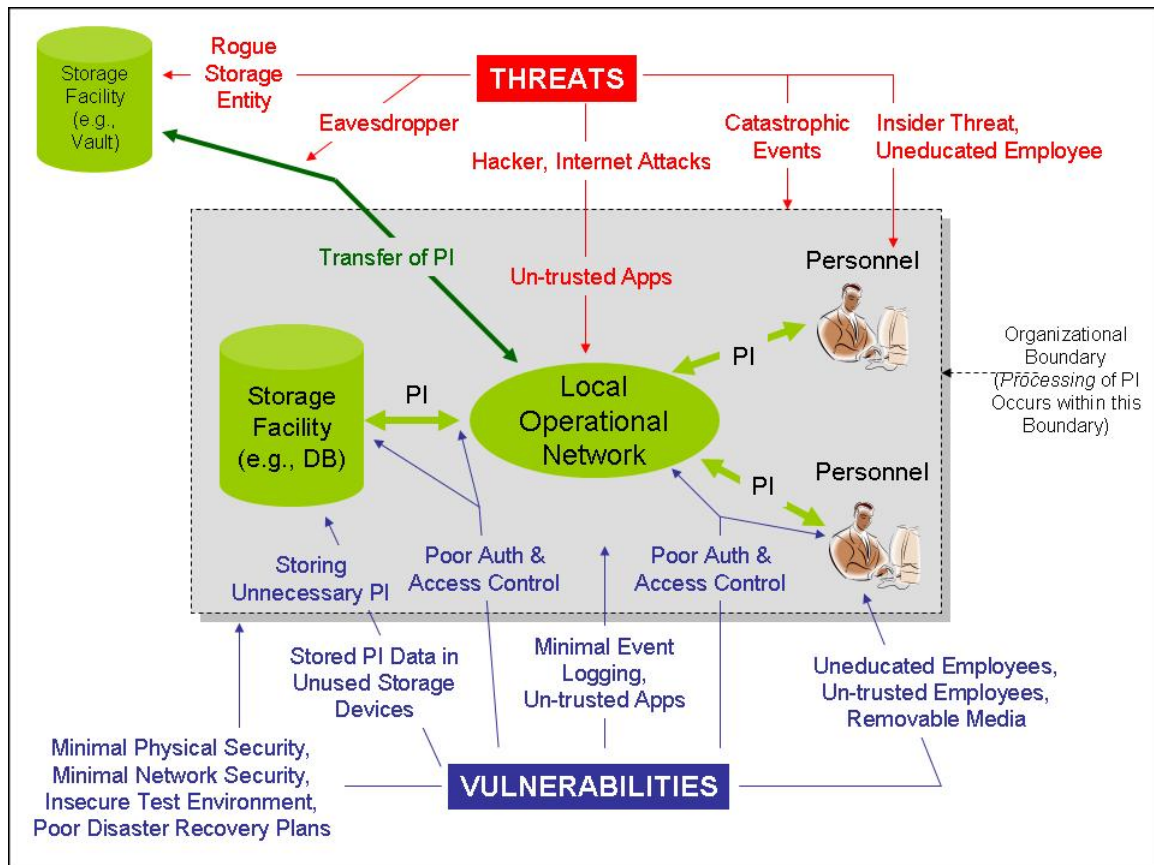


Figure 6: Storing PI (Locally and Remotely)

Threats:

- *Rogue Storage Entity* – An entity that poses to be a legitimate storage entity for the purposes of collecting PI.
- *Insider Threat* – An employee, contractor, etc., that has internal access to organizational assets, and intends to leverage that access to perform unauthorized functions.
- *Uneducated Employee* – An employee (or contractor) who unknowingly performs unauthorized functions (e.g., emailing PI over unprotected networks, screen prints of PI), is susceptible to social engineering attacks that disclose PI, or performs ill-advised functions due to lack of education (e.g., poor development and testing practices, inappropriate use of PI in testing environments).

- *Eavesdropper* – An entity that is capable of intercepting PI (without knowledge by the mortgage entity) as it is transferred to be stored.
- *Hacker* – An entity purposely attempting to gain unauthorized access to computer systems.
- *Internet-based Attack* – Worms, viruses, etc., that promulgate via the Internet and look to exploit vulnerabilities within computing networks and systems.
- *Un-trusted Applications* – Applications that perform functions they are not supposed to perform, or do not perform functions they are supposed to perform.
- *Catastrophic Events* – Unforeseen events (e.g., natural disasters, major power outages) that cause operations to cease.

#### Vulnerabilities:

- *Minimal Physical Security* – Minimal or poor physical security to prevent unauthorized access to critical computing equipment.
- *Minimal Network Security* – Minimal or poor enterprise network security at that leads to exposure of PI as it is being transferred. Specific vulnerabilities include:
  - Use of non-secure protocols (e.g., SQL, RPC)
  - No use of firewalls or poor configuration of firewalls
  - Out of date security patches on computing equipment
  - Unneeded cached PI data resident on computing equipment
  - Lack of intrusion detection / intrusion prevention capabilities
  - Poor key management to support cryptographic functions (e.g., SSH)
  - Insecure configuration of computing equipment, including lack of audit to verify configuration
  - Out of date virus detection capabilities
- *Removable Media* – Media such as USB drives, PDAs, notebook computers, etc., that can store PI and also be easily removed from the operational environment of the mortgage entity.
- *Stored PI Data in Unused Storage Devices* – Storage devices that are not in current use (e.g., retired, being repaired/serviced, damaged) but contain PI.
- *Minimal Event Logging* – Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
- *Insecure Test Environment* – Test environments that use “live operational data” but have lax security capabilities compared to the operational environments.
- *Poor Disaster Recovery Plans and Capabilities* – Plans and capabilities that do not exist, or exist but are in such poor condition that an organization is unable to recover back to adequate operating state after a catastrophic event has occurred.
- *Storing Unnecessary PI* – A mortgage entity that transfers additional PI that is not needed by the storage entity.
- *Poor Authentication & Access Control* – An inability to authenticate individuals and applications involved in storing PI (or accessing stored PI), as well as determining the privileges & authorizations of individuals and applications.
- *Uneducated Employee* – An employee (or contractor) who has little to no security awareness as it relates to the performance of his/her job, and specifically to the handling of PI.
- *Un-trusted Employee* – An employee (or contractor) performing in a trusted role (e.g., database administrator with access to PI) without having the necessary qualifications fulfilled for that trusted role (e.g., background check).
- *Un-trusted Applications* – Sensitive applications (i.e., that process PI) that do not meet specific security and trust requirements. Un-trusted applications may be due to:

- Poor requirements specification
- Poor development and coding practices
- Poor testing practices
- Complexity within the application

Table 4 provides a mapping of threats to vulnerabilities, and also defines the resultant risk for when threats exploit vulnerabilities while PI is being stored.

**Table 4: Storing PI Threats and Vulnerabilities**

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
Rogue Storage Entity	Poor Authentication & Access Control	Rogue entity gains access to PI that is being transferred to the rogue entity.
	Storing Unnecessary PI	Rogue entity gains more PI than originally anticipated.
	Minimal Event Logging	Rogue entity's actions go unnoticed by the valid mortgage entity transferring PI to the rogue storage entity.
	Uneducated Employee	Rogue entity is able to socially engineer an employee into storing PI at the rogue entity.
	Un-trusted Employee	Rogue entity corroborates with un-trusted employee in obtaining transferred PI for storage at the rogue entity.
Internet-based Attack	Minimal Network Security	Worm, virus, etc., is capable of penetrating enterprise storage systems and causing applications to disclose PI.
	Minimal Event Logging	Internet attack goes unnoticed by mortgage entity, or is noticed after PI has been disclosed.
	Uneducated Employee	Employee is socially engineered (e.g., phishing) into launching an Internet attack within the enterprise with the intent to disclose PI.
	Un-trusted Application	Internet attack leverages a known vulnerability (i.e., an un-trusted process) in a product or application to disclose PI.
	Insecure Test Environment	Worm, virus, etc., is capable of penetrating test environment causing the disclosure of PI.
Insider Threat	Minimal Network Security	Insider gains easy network access to mortgage entity storage systems containing PI.
	Minimal Physical Security	Insider gains easy physical access to mortgage entity storage systems containing PI.
	Minimal Event Logging	Insider's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Insider is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Insider corroborates with un-trusted employee in gaining access to systems containing PI.
	Insecure Test Environment	Insider gains access to PI that is resident in the test environment.
	Un-trusted Applications	Insider is able to determine that applications perform certain un-trusted functions (e.g.,

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
		disclosing PI), and leverages those applications in obtaining PI.
	Removable Media	Insider uses media that is easily removed from the operational environment to store PI for the purpose of using/distributing the PI in an unauthorized manner.
	Stored PI Data in Unused Storage Devices	Insider accesses these unused storage devices to obtain PI that is still resident on those devices.
Hacker	Poor Authentication & Access Control	Hacker gains access to PI that is resident on storage systems.
	Minimal Network Security	Hacker gains access to mortgage entity storage systems containing PI.
	Minimal Event Logging	Hacker's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Hacker is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Hacker corroborates with un-trusted employee in gaining access to systems containing PI.
	Un-trusted Applications	Hacker is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications in obtaining PI.
	Insecure Test Environment	Hacker gains access to PI that is resident in the test environment.
Uneducated Employee	Uneducated Employee	An employee with little to no security awareness or training is a threat waiting to exploit its own vulnerability. These employees typically do not understand the importance for protecting PI, and in basic terms "don't know what they don't know." They perform activities that typically involve providing PI to anyone who claims a need to have it.
	Minimal Event Logging	Uneducated employee's (accidental) activities in disclosing PI go unnoticed by mortgage entity.
	Removable Media	Employee unknowingly removes media containing PI from operational environment. The media is now susceptible for compromise.
	Stored PI Data in Unused Storage Devices	Employee unknowingly provides/uses these types of storage devices that contain PI (e.g., takes it in for repair, takes it home for personal use). The device is now susceptible for compromise.
Un-trusted Applications	Un-trusted Applications	Similar to uneducated employees, un-trusted applications can be a threat waiting to exploit their own vulnerabilities. Due to lack of testing, poor development practices, etc., these applications perform functions that are not supposed to be performed, and vice-versa, which

Threat	Vulnerability	Risk
		can lead to disclosure of PI.
	Minimal Event Logging	Un-trusted application's (unanticipated) activities in disclosing PI go unnoticed by mortgage entity.
Catastrophic Event	Poor Disaster Recovery Plans and Capabilities	If disaster recovery and business continuity plans and capabilities do not provide for an operational environment that is as secure as the original operating environment, then all the above threats, vulnerabilities and exploitations apply to the environment operating in disaster recovery mode.
Eavesdropper	Minimal Network Security	Eavesdropper is capable of intercepting PI that is poorly protected, or not protected at all (e.g., weak cryptography, insecure protocols) while it is being transferred for storage.
	Storing Unnecessary PI	Eavesdropper gains more PI than originally anticipated.

### 3.1.5. Disposing Personal Information

#### 3.1.5.1. Definition

*Disposing* – Disposing PI is the deletion or discarding of personal information that is no longer needed within an electronic mortgage process or function. Personal information can be deleted or discarded from both temporary and long term containers.

#### 3.1.5.2. Threats and Vulnerabilities

Figure 7 represents a general use case where PI is being stored, locally as well as remotely. Within this use case, common threats and vulnerabilities are highlighted.

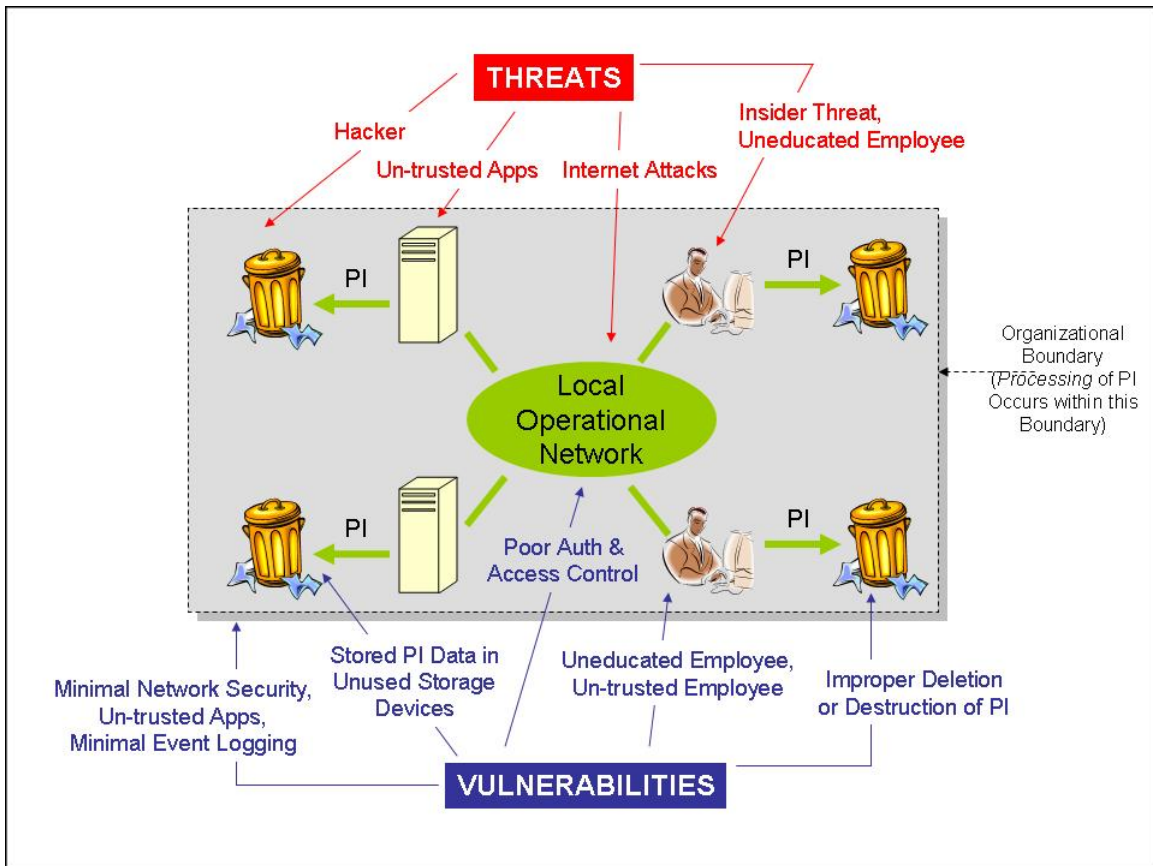


Figure 7: Disposing PI within a Mortgage Entity

Threats:

- *Hacker* – An entity purposely attempting to gain unauthorized access to computer systems.
- *Internet-based Attack* – Worms, viruses, etc., that promulgate via the Internet and look to exploit vulnerabilities within computing networks and systems.
- *Insider Threat* – An employee, contractor, etc., that has internal access to organizational assets, and intends to leverage that access to perform unauthorized functions.
- *Uneducated Employee* – An employee (or contractor) who unknowingly performs unauthorized functions (e.g., improperly disposing of PI), is susceptible to social engineering attacks that disclose PI, or performs ill-advised functions due to lack of education (e.g., poor development practices in deleting sensitive data).
- *Un-trusted Applications* – Applications that perform functions they are not supposed to perform, or do not perform functions they are supposed to perform.

Vulnerabilities:

- *Minimal Network Security* – Minimal or poor enterprise network security at that leads to exposure of PI as it is being transferred. Specific vulnerabilities include:
  - Use of non-secure protocols (e.g., SQL, RPC)
  - No use of firewalls or poor configuration of firewalls
  - Out of date security patches on computing equipment
  - Unneeded cached PI data resident on computing equipment
  - Lack of intrusion detection / intrusion prevention capabilities
  - Poor key management to support cryptographic functions (e.g., SSH)

- Insecure configuration of computing equipment, including lack of audit to verify configuration
- Out of date virus detection capabilities
- *Minimal Event Logging* – Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
- *Stored PI Data in Unused Storage Devices* – Storage devices that are not in current use (e.g., retired, being repaired/serviced, damaged) but contain PI.
- *Poor Authentication & Access Control* – An inability to authenticate individuals and applications involved in storing PI (or accessing stored PI), as well as determining the privileges & authorizations of individuals and applications.
- *Uneducated Employee* – An employee (or contractor) who has little to no security awareness as it relates to the performance of his/her job, and specifically to the handling of PI.
- *Un-trusted Employee* – An employee (or contractor) performing in a trusted role (e.g., database administrator with access to PI) without having the necessary qualifications fulfilled for that trusted role (e.g., background check).
- *Un-trusted Applications* – Sensitive applications (i.e., that process PI) that do not meet specific security and trust requirements. Un-trusted applications may be due to:
  - Poor requirements specification
  - Poor development and coding practices
  - Poor testing practices
  - Complexity within the application
- *Improper Deletion or Destruction of PI* – PI that is still resident within the system even after disposal procedures have been followed (e.g., not wiping hard disks containing PI).

Table 5 provides a mapping of threats to vulnerabilities, and also defines the resultant risk for when threats exploit vulnerabilities while PI is being disposed.

**Table 5: Disposing PI Threats and Vulnerabilities**

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
Internet-based Attack	Minimal Network Security	Worm, virus, etc., is capable of penetrating enterprise systems and causing applications to disclose PI.
	Minimal Event Logging	Internet attack goes unnoticed by mortgage entity, or is noticed after PI has been disclosed.
	Uneducated Employee	Employee is socially engineered (e.g., phishing) into launching an Internet attack within the enterprise with the intent to disclose PI.
	Un-trusted Application	Internet attack leverages a known vulnerability (i.e., an un-trusted process) in a product or application to disclose PI.
	Improper Deletion or Destruction of PI	Internet attack gains access to and exposes PI that is believed to have been deleted or destroyed.
Insider Threat	Minimal Network Security	Insider gains easy network access to mortgage entity storage systems containing PI.
	Minimal Event Logging	Insider's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Insider is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.

<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
	Un-trusted Employee	Insider corroborates with un-trusted employee in gaining access to systems containing PI.
	Un-trusted Applications	Insider is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications in obtaining PI.
	Improper Deletion or Destruction of PI	Insider gains access to PI that is believed to have been deleted or destroyed.
	Stored PI Data in Unused Storage Devices	Insider accesses these unused storage devices to obtain PI that is still resident on those devices.
Hacker	Poor Authentication & Access Control	Hacker gains access to PI that is resident on storage systems.
	Minimal Network Security	Hacker gains access to mortgage entity storage systems containing PI.
	Minimal Event Logging	Hacker's activities in obtaining PI go unnoticed by mortgage entity.
	Uneducated Employee	Hacker is able to socially engineer an employee into disclosing PI, or information that leads to the disclosure of PI.
	Un-trusted Employee	Hacker corroborates with un-trusted employee in gaining access to systems containing PI.
	Un-trusted Applications	Hacker is able to determine that applications perform certain un-trusted functions (e.g., disclosing PI), and leverages those applications in obtaining PI.
	Improper Deletion or Destruction of PI	Hacker gains access to PI that is believed to have been deleted or destroyed.
Uneducated Employee	Uneducated Employee	An employee with little to no security awareness or training is a threat waiting to exploit its own vulnerability. These employees typically do not understand the importance for protecting PI, and in basic terms "don't know what they don't know." They perform activities that typically involve providing PI to anyone who claims a need to have it.
	Minimal Event Logging	Uneducated employee's (accidental) activities in disclosing PI go unnoticed by mortgage entity.
	Improper Deletion or Destruction of PI	Employee improperly disposes of PI such that the PI is still resident within the system and can be compromised.
	Stored PI Data in Unused Storage Devices	Employee improperly disposes of these devices that contain PI such that the PI is still resident within the device and can be compromised.
Un-trusted Applications	Un-trusted Applications	Similar to uneducated employees, un-trusted applications can be a threat waiting to exploit their own vulnerabilities. Due to lack of testing, poor development practices, etc., these applications perform functions that are not

Threat	Vulnerability	Risk
		supposed to be performed, and vice-versa, which can lead to disclosure of PI.
	Minimal Event Logging	Un-trusted application's (unanticipated) activities in disclosing PI go unnoticed by mortgage entity.
	Improper Deletion or Destruction of PI	Application improperly disposes of PI such that the PI is still resident within the system and can be compromised.

### 3.2. Recommended Policies and Procedures

This section provides recommended policies and procedures for the vulnerabilities identified in section 3.1 (see Table 6). Many of the vulnerabilities identified in the previous section apply to more than one use case; therefore, a general summary of these recommended policies and procedures is provided in a consolidated form within this section. Any recommendations that differ based on the specific type of threat related to a particular vulnerability are noted below.

**Table 6: Recommended Policies and Procedures for Managing PI**

Vulnerability	Recommended Policies and Procedures
Poor Authentication	Perform an assurance assessment on PI assets, and applications that manage PI assets, to determine the level of authentication assurance required for those assets and applications. Assurance requirements are typically categorized as low, medium and high assurance, where higher assurance requirements dictate stronger authentication solutions. <sup>7</sup>
Poor Access Control	<p>Define security policy requirements that assign <i>roles</i> to <i>entities</i>, and <i>privileges (authorizations)</i> to <i>roles</i>, thereby enforcing <i>privileges</i> on <i>entities</i>. A well accepted standard for developing role-based access control (RBAC) solutions for enterprise environments is ANSI/INCITS 359.<sup>8</sup> In addition, NIST Special Publication 800-53 includes a detailed section on access control security controls.<sup>9</sup></p> <p>Access control answers the question: “Who/what is allowed to access an asset, or perform a function?” In terms of PI, this means “who/what is allowed to access/view PI?” or “who/what is allowed to perform a certain function using data that is PI?” By defining specific <i>roles</i> in your enterprise (e.g., loan origination officer, loan processor) as well as specific <i>privileges</i> that are tied to those roles (e.g., view PI, transfer PI), applications can be deployed that 1) check an <i>entity's role</i> at logon and 2) ensure that the <i>privileges</i> defined for that <i>role</i> correspond to the <i>actions</i> being performed by the <i>entity</i>. The solution is elegant in that an enterprise can separate</p>

<sup>7</sup> NIST Special Publication 800-63 is an excellent resource for understanding authentication assurance levels and appropriate technologies for those assurance levels. The NIST publication can be located at [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6\\_3\\_3.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf). For organizations deciding to use PKI, SISAC provides information on certificate assurance levels applicable to the mortgage industry. See <http://www.sisac.org>.

<sup>8</sup> Information on ANSI/INCITS 359, as well as general information on RBAC can be found at <http://csrc.nist.gov/rbac/rbac-stds-roadmap.html>.

<sup>9</sup> <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>

Vulnerability	Recommended Policies and Procedures
	the management of <i>roles/privileges</i> from <i>roles/entities</i> , and it does not require each <i>entity</i> to have a specific set of <i>privileges</i> defined for that <i>entity</i> .
Minimal Event Logging	Define security policy requirements for information systems that handle PI to have audit and event logging capabilities installed and operating. Audit logs are typically detailed and used for forensic analysis; event logs can be tailored to notify an organization of certain events that occur in a system (e.g., x number of unsuccessful logon attempts to a computer system), and are typically categorized as low, medium or high security events. Appendix F of NIST Special Publication 800-53 provides recommendations for specific audit and accountability requirements that can be implemented within an organization. In addition, the Information Systems Audit and Control Association (ISACA) has defined the Information System Auditing Guideline for Privacy. <sup>10</sup>
Collecting / Transferring / Storing Unnecessary PI	Perform an assessment on PI required to support your organization's mortgage related functions, as well as an assessment on the PI that your organization is actually collecting/transferring/storing. Ensure that the PI being collected/transferred/stored is no more than the PI needed to support your organization's mortgage related functions. In addition, train staff on the types of PI that are required to be collected/transferred/stored vs. PI that is not required to be collected/transferred/stored. For PI transfers and remote storage operations, ensure that your business partners and other third party organizations have security requirements for transferring/storing PI similar to your own requirements. In some cases, your organization may want to ask for an audit to ensure your partners have implemented appropriate security controls.
Minimal Physical Security (Mortgage Entity Enterprise)	Perform an assessment on each physical location containing information systems that process PI to determine the appropriate level of physical protection needed at those locations (e.g., guards, badging systems, alarms, entry/exit log book).
Minimal Network Security (Mortgage Entity Enterprise)	Perform an assessment on each information system that collects PI to determine the appropriate confidentiality and data integrity requirements for the PI. By examining PI and the information systems that collect PI, your organization can determine the level of confidentiality and data integrity required for the PI and those information systems. NIST FIPS 199 <sup>11</sup> and ISO 17799 <sup>12</sup> are excellent resources for performing this type of assessment.
Minimal Security (Consumer Computing Equipment)	Provide educational material on a periodic basis to your consumer community to help them stay abreast of computer and Internet security issues, and how they can better protect themselves and enhance their on-line experience with your organization.
Minimal Security /	Define policy requirements that require all PI to be encrypted

<sup>10</sup><http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18651>

<sup>11</sup><http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

<sup>12</sup><http://www.iso-17799.com/>

Vulnerability	Recommended Policies and Procedures
Insecure Transfer Methods (Allows Eavesdropper to Steal PI)	<p>(preferably using NIST FIPS approved encryption algorithms, e.g., AES)<sup>13</sup> when being transmitted over public networks or other similar insecure environments (e.g., physical media).</p> <p>Define policy requirements that require monitoring of PI being transmitted, and ensuring that PI is transmitted over secured communication channels.</p>
Poor Authentication (Rogue Web Site)	<p>Provide educational material on a periodic basis to your consumer community to help them differentiate between a rogue web site attempting to resemble your web site, and your real operational web site. Clarify to your consumers how you will communicate with them, and how to successfully verify that they are visiting your web site, and not a malicious one. For proper authentication of SSL protected web sites, reference SISAC's recommendations.<sup>14</sup></p>
Removable Media	<p>Define acceptable forms of removable media based on your operational environment, and specifically, the risks identified in your operational environment that relate to the unauthorized disclosure of PI. In highly risky environments, organizations may want to consider banning removable media to ensure PI is not easily removed from the environment. Providing educational material to employees informing them of the risks associated with removable media is also helpful. Employees need to understand that they may inadvertently place PI on removable media, and then remove that media from the intended operational environment.</p>
Stored PI in Unused Storage Devices / Improper Deletion or Destruction of PI	<p>Define a set of procedures for properly disposing of devices that are no longer needed but contain PI, or completely and securely deleting the PI from the devices if the devices are to be reused at a later time. The procedures should include the definition of personnel who are authorized to execute such procedures (see access control roles and privileges).</p>
Uneducated Consumer	<p>Provide educational material<sup>15</sup> on a periodic basis to your consumer community to help them stay abreast of computer and Internet security issues, and how they can better protect themselves and enhance their on-line experience with your organization. Educational material should include information on the need to implement technical solutions (e.g., virus protection) as well as to be aware of social engineering based attacks (e.g., phishing emails). In addition, display your organization's policies and practices regarding protection of personal information to your consumers so they understand how you will securely manage their personal information.</p>
Un-trusted Employee	<p>Identify <i>trusted roles</i> (see access control) for sensitive operational environments and applications. Trusted roles should be fulfilled by highly trusted employees. Background checks are a typical practice to ensure the person fulfilling the trusted role is credible and has a</p>

<sup>13</sup> FIPS 197 defines AES and can be found at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

<sup>14</sup> <http://www.sisac.org>

<sup>15</sup> Reference BITS Consumer Confidence Toolkit: Data Security and Financial Services located at <http://www.bitsinfo.org/downloads/Publications%20Page/bitscons2005.pdf>

Vulnerability	Recommended Policies and Procedures
	reputable background. In addition, organizations can employ the concept of a “no-lone zone” to ensure that at least two trusted personnel are present to perform sensitive operations.
Uneducated Employee	Provide educational material and seminars on a periodic basis to your employees to help them stay abreast of computer and Internet security issues, and to understand their responsibilities in performing their security related functions and the importance of those activities to the company and the consumer. There are many training programs available in the marketplace. To select the appropriate program for your enterprise, first assess what your organization needs in terms of training and education, and then prepare yourself with a list of questions you would like answered by potential trainers to ensure they are addressing your specific needs. In addition, BITS has defined a set of recommended success criteria for implementing and executing security awareness training programs. <sup>16</sup>
Super User	Minimize the need for Super User roles within your enterprise to avoid having one employee be assigned many roles with many privileges. These users have access to many types of information, and they pose a threat to the organization should they be influenced to perform unauthorized functions that exploit their having many roles & privileges.
Un-trusted Application	Identify those applications that perform sensitive functions (e.g., processing PI), and enforce a software development, test and deployment method that ensures those applications only perform as defined by the application’s requirements. More specifically, these applications should only perform what they are supposed to perform, and not perform anything they are not supposed to perform. A well-known model for ensuring the use of mature and tested applications in your environment is the Capability Maturity Model for Software (SW-CMM) developed by the Software Engineering Institute (SEI) at Carnegie-Mellon. <sup>17</sup> Although the model is no longer being maintained, there is still useful information available to assist organizations in maturing their applications and processes to ensure a more trusted operating environment.
Non-compliant 3 <sup>rd</sup> Party Service Provider	Ensure that your business partners and other third party organizations have defined and implemented security policies and requirements for managing PI that are similar to your own policies and requirements. In some cases, your organization may want to ask for an audit to ensure your partners have implemented appropriate security controls. BITS has published a recommended framework specifically for managing risk associated with service providers. <sup>18</sup>
Insecure Test Environment	Define security requirements for your application testing environment that are similar (if not exact) to your operational environment. In addition, define requirements that prohibit testing with live, operational data unless absolutely necessary. Insecure

<sup>16</sup> <http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf>

<sup>17</sup> <http://www.sei.cmu.edu/cmm/>

<sup>18</sup> BITS Framework for Managing Technology Risk for IT Service Provider Relationships located at <http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf>

Vulnerability	Recommended Policies and Procedures
	testing environments (especially ones that test with operational data) are targets for hackers and other adversaries due to the ease in which these adversaries can gain access into these environments and extract operational data such as PI. Use of standards such as SEI's SW-CMM (as noted above) or other similar best practices for testing environments should be enforced within organizations.
Poor Disaster Recovery Plans and Capabilities	Dedicate time and effort to implement and test effective disaster recovery plans. The CIO Executive Council has published their <i>Eight Best Practices for Disaster Recovery</i> <sup>19</sup> , which can be used by an organization's CIO or executive management.

### 3.3. Recommended Security Technologies

This section provides recommended security technologies for the vulnerabilities identified in section 3.1 (see Table 7). Many of the vulnerabilities identified in the previous section apply to more than one use case; therefore, a general summary of these recommended security technologies is provided in a consolidated form within this section. Any recommendations that differ based on the specific type of threat related to a particular vulnerability are noted below.

**Table 7: Recommended Security Technologies for Managing PI**

Vulnerability	Recommended Security Technologies
Poor Authentication	Based on the results of the authentication assurance assessment discussed in the previous section, appropriate authentication technologies include passwords, PINs, authentication tokens, digital certificates, smart cards, knowledge-based authentication, biometrics, and multi-factor authentication tokens. Passwords and PINs are typically associated with lower assurance needs, while digital certificates, smart cards and multi-factor authentication tokens are associated with higher assurance needs. NIST SP 800-63 and SISAC are excellent resources in determining which authentication technology is appropriate based on a pre-determined authentication assurance level.
Poor Access Control	There are a variety of access control technologies and products in the marketplace today. Selecting one is dependent on 1) the technologies already deployed in your operational environment, 2) the results of your access control assessment performed as part of your policies and procedures activities, and 3) the type of authentication scheme you will employ, as access control functions are dependent on an authentication function being performed first. Various types of access control technologies include: <ul style="list-style-type: none"> <li>• <i>PKI Certificate Based Access Control</i> – Access control performed based on the information defined within an X.509 PKI certificate.<sup>20</sup> X.509 certificate support is available in many commercial products.</li> <li>• <i>Security Assertion Markup Language (SAML)</i> – XML based</li> </ul>

<sup>19</sup> <http://www.cio.com/archive/111504/exchange.html>

<sup>20</sup> RFC 3280 defines standard contents typically founding X.509 certificates. This standard can found at <http://www.ietf.org/rfc/rfc3280.txt>.

Vulnerability	Recommended Security Technologies
	<p>protocol that asserts authorization and privilege information about an entity.<sup>21</sup> SAML is widely supported in many commercial products.</p> <ul style="list-style-type: none"> <li>• <i>Liberty Alliance</i> – The Liberty Alliance is a consortium representing organizations from around the world to address the technical, business, and policy challenges around identity and identity based Web services. SAML is a core component of their technology framework.<sup>22</sup> Many commercial products provide support for both Liberty 1.0 and 2.0 specifications.</li> <li>• <i>Web Services Security (WS-Security)</i> – WS-Security is a standard co-developed by Microsoft, IBM and VeriSign that provides a general-purpose mechanism for associating security tokens with messages.<sup>23</sup> WS-Security support is predominantly available in Microsoft’s product offerings.</li> <li>• <i>Shibboleth</i> – An academia developed solution for providing secured online services or access restricted digital content.<sup>24</sup></li> </ul>
Minimal Event Logging	Most computing equipment comes with built-in audit and event logging capabilities. Ensure that these capabilities are turned on and operating, and customized appropriately to meet your organization’s security policy requirements.
Collecting / Transferring / Storing Unnecessary PI	<p>There are no specific security technologies that apply to this vulnerability, but your organization can perform the following functions with respect to technologies used in collecting/transferring/storing PI:</p> <ul style="list-style-type: none"> <li>• Ensure web pages and other user interfaces that are used to collect PI are structured to only collect PI that is required by the intended application</li> <li>• Where possible, perform data checking (e.g., on receipt of collected PI) on PI to ensure that the correct PI has been collected, transferred or stored</li> </ul>
Minimal Physical Security (Mortgage Entity Enterprise)	<p>Security technologies that can be applied to a physical environment include:</p> <ul style="list-style-type: none"> <li>• ID badging systems (contact and contactless)</li> <li>• Biometric scanning systems</li> </ul>
Minimal Network Security (Mortgage Entity Enterprise)	<p>Recommended security technologies for your organization’s enterprise security include:</p> <ul style="list-style-type: none"> <li>• Firewalls for perimeter security and protocol/application level access control to ensure only authorized protocols and applications are allowed access into your enterprise environment;</li> <li>• Patch management capabilities to ensure the most recent security patches are installed and operating on your computing systems;</li> </ul>

<sup>21</sup> Information on SAML can be found at <http://www.xmltrustcenter.org/saml/index.htm>.

<sup>22</sup> Information on the Liberty Alliance can be found at <http://www.projectliberty.org/>.

<sup>23</sup> Information on V1.0 of WS-Security can be found at <http://www.verisign.com/wss/wss.pdf>.

<sup>24</sup> Information on the Shibboleth Project can be found at <http://shibboleth.internet2.edu/>.

Vulnerability	Recommended Security Technologies
	<ul style="list-style-type: none"> <li>• Virus protection to ensure Internet/computer viruses do not propagate undetected throughout your environment;</li> <li>• Intrusion detection/prevention capabilities to both detect and alert when a security relevant intrusion occurs, as well as to potentially stop an intrusion from occurring;</li> <li>• Authentication &amp; access control to provide strict enforcement over who/what has authorized access to personal information assets; and,</li> <li>• Encryption to ensure personal information at rest cannot be read in its plaintext form should an unauthorized entity gain access to the information.</li> </ul> <p>To some degree, each of these security technologies should be implemented within your organization, as they each address different security issues. The degree to which your organization implements these technologies is determined based on the security assessment performed using resources such as FIPS 199 and ISO 17799 as guidance. Additional guidance is provided in NIST SP 800-53.</p>
Minimal Security (Consumer Computing Equipment)	Educate the consumers to promote installation and operation of personal/home-use firewalls and virus protection software on consumer computing equipment.
Minimal Security / Insecure Transfer Methods (Allows Eavesdropper to Steal PI)	<p>For PI being transmitted over the Internet, organizations should require the use of SSL/TLS<sup>25</sup> or IPSEC<sup>26</sup> (with minimum 128 bit encryption) to encrypt the PI being transmitted.</p> <p>For email containing PI, email should be encrypted using an application that implements the S/MIMEv3<sup>27</sup> specification. Pretty Good Privacy (PGP) encryption is also a well-known and used solution for encrypting email. The IETF is updating the OpenPGP standard<sup>28</sup>, and additional information on PGP can be found at <a href="http://www.pgp.com">www.pgp.com</a>.</p> <p>For PI being transmitted via physical media, organizations should require encryption of the PI on that media using a NIST FIPS approved algorithm (e.g., AES).</p> <p>Consider implementation of security devices that support monitoring or filtering of data to ensure that data such as PI are not transmitted over insecure communication channels.</p> <p>SSL/TLS, IPSEC and S/MIMEv3 are standards currently supported in many commercial product offerings.</p>
Poor Authentication	Organizations should implement SISAC organizational device

<sup>25</sup> <http://www.ietf.org/rfc/rfc2246.txt>

<sup>26</sup> Information on the IPSEC protocol suite can be found at <http://www.networksorcery.com/enp/topic/ipsecsuite.htm>.

<sup>27</sup> The S/MIMEv3 specification is defined in <http://www.ietf.org/rfc/rfc2633.txt> and the S/MIMEv3.1 specification is defined in <http://www.ietf.org/rfc/rfc3851.txt>.

<sup>28</sup> <http://www.ietf.org/internet-drafts/draft-ietf-openpgp-rfc2440bis-15.txt>

<b>Vulnerability</b>	<b>Recommended Security Technologies</b>
(Rogue Web Site)	certificates to authenticate mortgage industry web sites. See sections 3.1.8 and 3.1.10 of SISAC's Certificate Policy Requirements Document (CRPD). <sup>29</sup>
Removable Media	For removable media stored in medium to high risk operational environments (i.e., the media is at risk of being removed from the environment in an unauthorized fashion and contains PI), the contents on the removable media should be encrypted using a NIST FIPS approved algorithm (e.g., AES) with minimum 128 bit security.
Stored PI in Unused Storage Devices / Improper Deletion or Destruction of PI	There are many commercial products available in the marketplace that are capable of performing a "secure delete" or "secure wipe" of information and data contained in media and other storage devices. Organizations should research these product offerings based on their specific requirements and security assessments to determine which product offering is best suited for their environment.
Uneducated Consumer	Not applicable to technology. See Uneducated Consumer in Table 6.
Un-trusted Employee	Not applicable to technology. See Un-trusted Employee in Table 6.
Uneducated Employee	Not applicable to technology. See uneducated Employee in Table 6.
Super User	See Authentication and Access Control above.
Un-trusted Application	Not applicable to technology. See Un-trusted Application in Table 6.
Non-compliant 3 <sup>rd</sup> Party Service Provider	Not applicable to technology. See Non-compliant 3 <sup>rd</sup> Party Service Provider in Table 6.
Insecure Test Environment	Not applicable to technology. See Insecure Test Environment in Table 6.
Poor Disaster Recovery Plans and Capabilities	Not applicable to technology. See Poor Disaster Recovery Plans and Capabilities in Table 6.

### 3.4. Recommended Incident Response Plans

This section provides recommended incident response plans for when PI is disclosed in an unprotected form to unauthorized entities. These recommendations are based on those outlined by the California Office of Privacy Protection (COPP),<sup>30</sup> as well as those defined in NIST SP 800-61<sup>31</sup> and can be applied to any of the use cases identified in section 3.1 and tailored specifically to meet your organization's needs.

At a minimum, it is recommended that organizations define incident response plans to include the following general activities:

- Monitoring and notification of a security incident involving the unauthorized disclosure of PI
- Impact assessment of the security incident
- Internal notification procedures
- External notification procedures

<sup>29</sup> <http://www.sisac.org/documents/SISACCertPolicyReqsDocv14.pdf>.

<sup>30</sup> <http://www.privacy.ca.gov/recommendations/secbreach.pdf>

<sup>31</sup> <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

- Follow-up assessment to mitigate the security incident from recurring and update to incident response plans

Furthermore, your organization should define a specific team of individuals who has the responsibility for executing and managing your incident response plans. NIST SP 800-61 defines three general types of incident response team structures: Central Incident Response Team, Distributed Incident Response Teams, and Coordinating Team. The type of team your organization selects will depend on how your organization is structured and how to best communicate incident response actions.

**Central Incident Response Team.** A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for large organizations with minimal geographic diversity in terms of computing resources.

**Distributed Incident Response Teams.** The organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents. Strong communication among teams and consistent practices should make incident handling more effective and efficient.

**Coordinating Team.** An incident response team provides guidance and advice to other teams without having authority over those teams – for example, an organization-wide team may assist individual departments’ teams. This model can be thought of as an incident response team for other incident response teams.

### 3.4.1. Incident Monitoring and Notification

Once your organization has identified the information systems where PI resides, monitoring capabilities can be applied to provide alerts when potential security incidents occur. According to NIST SP 800-61, signs of an incident fall into two categories: indications and precursors. A *precursor* is a sign that an incident may occur in the future. An *indication* is a sign that an incident may have occurred or may be occurring now. Precursors and indications are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people. See section 3.2.3 of 800-61 for additional information.

### 3.4.2. Impact Assessment

Should a security incident involving the potential unauthorized disclosure of PI occur, your incident response team should first perform an initial assessment of the incident to determine its overall impact on your organization as well as to anyone outside of your organization.

Assessment should include:

- Whether or not PI had actually been disclosed
- How much PI may have been disclosed
- The type of PI that may have been disclosed
- To whom the PI may have been disclosed to

- If the PI was disclosed, was it protected (e.g., encrypted)

Care should be taken in understanding what exactly defines a security incident. Due to the amount of logging capabilities that exist in computing equipment, an organization can spend a large amount of time examining and assessing incidents. Therefore, the better your personnel understand normal behavior in your operational environment, the better trained they will be in responding to and assessing the impacts of security incidents.

### 3.4.3. Internal Notification

To ensure that notification is performed successfully, correctly and consistently, organizations should identify a single individual responsible for notifying the appropriate personnel within the organization when the incident response team has determined that PI may have been disclosed. From section 2.4.4 of SP 800-61, internal personnel that may need to be notified include:

**Management.** Management invariably plays a pivotal role in incident response. In the most fundamental sense, management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to other parties. Without management support, an incident response team is unlikely to be successful.

**Information Security.** Members of the information security team are often the first to recognize that an incident has occurred or is occurring and may perform the initial analysis of incidents. In addition, information security staff members may be needed during other stages of incident handling—for example, altering network security controls (e.g., firewall rule-sets) to contain an incident.

**Telecommunications.** Some incidents involve unauthorized access to telephone lines, such as dialing into unsecured modems. Private Branch Exchange (PBX) compromises often are intertwined with break-ins into other systems. The telecommunications staff is aware of the current capabilities and the Points of Contacts (POCs) and procedures for working with telecommunications carriers.

**IT Support.** IT technical experts (e.g., system administrators, network administrators, and software developers) not only have the needed technical skills to assist during an incident but also usually have the best understanding of the technology with which they deal on a daily basis. This understanding can facilitate decisions such as whether to disconnect an attacked system from the network.

**Legal Department.** Legal experts should review incident response policies and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit.

**Public Affairs and Media Relations.** Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public (within the constraints imposed by security and law enforcement interests).

**Human Resources.** When an employee is the apparent target of an incident or is suspected of causing an incident, the human resources department often becomes involved—for example, in assisting with disciplinary proceedings or employee counseling.

**Business Continuity Planning.** Computer security incidents undermine the business resilience of an organization and act as a barometer of its level of vulnerabilities and the inherent risks. Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to certain types of incidents, such as a denial of service (DoS). Organizations should also ensure that incident response policies and procedures and business continuity processes are in sync.

**Physical Security and Facilities Management.** Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. Threats made against the organization may not indicate whether logical or physical resources are being targeted. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office. Thus, close coordination between physical security and facilities management and the incident response team is important.

Determining who should be notified based on the type of security incident is left as an exercise for the organization to perform as part of its security policy development and incident response planning activities.

#### **3.4.4. External Notification**

In some cases, entities outside the organization may need to be notified, based on the impact assessment of a security incident. From the COPP recommendations and SP 800-61, these entities include:

**Owner of Personal Information.** Some state laws require the individual consumer to be notified if their PI has been disclosed in an unauthorized manner.

**Law Enforcement.** If your organization believes that a security incident may involve illegal activities, report it to appropriate law enforcement agencies. Your incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected.

**The Media.** Dealing with the media is an important part of incident response. The incident handling team should establish media communications procedures that are in compliance with the organization's policies on appropriate interaction with the media and information disclosure. Organizations often find it beneficial to designate a single media point of contact (POC) and at least one backup contact for discussing incidents with the media. Ideally, all members of the incident response team should be prepared to interact with the media.

**Incident Reporting Organizations.** Your organization may consider reporting security incidents to an independent 3<sup>rd</sup> party organization responsible for collecting and analyzing incident information. These institutions in turn provide benefits back to reporting organizations, such as security trends and incident alerts.

**Other Outside Parties.** Depending on the type of security incident, other parties include your organization's Internet Service Provider (ISP), other organizations from where a

security incident may have originated, software and hardware vendors, other incident response teams, and any other potentially affected parties.

As was the case for defining internal notification requirements, determining who should be notified externally is left as an exercise for the organization to perform as part of its security policy development and incident response planning activities.

### 3.4.5. Follow-Up Assessment

If a security incident should occur, it is critical to perform a follow-up assessment on the incident to understand why the incident occurred, and what steps can be taken in the future to mitigate the incident from occurring again. Your organization's incident response team should be responsible for performing this function, and updating your organization's incident response plans appropriately. From SP 800-61, there are three basic steps that should be performed as part of follow-up assessment:

**Lessons Learned.** One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handling process itself.

**Using Collected Incident Data.** Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team. Furthermore, organizations (e.g., Federal agencies) that are required to report incident information will need to collect the necessary data to meet their requirements.

**Evidence Retention.** Organizations should establish policy for how long evidence from an incident should be retained. Most organizations choose to retain all evidence for months or years after the incident ends. The following factors should be considered during the policy creation:

**Prosecution.** If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished.

**Data Retention.** Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that e-mail messages should be retained for only 180 days. If a disk image contains thousands of e-

mails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary.

**Cost.** Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and other devices that are used to hold disk images are individually inexpensive for most organizations. However, if an organization stores dozens of such components for years, the cost can be substantial. The organization also must retain functional computers that can use the stored hardware (e.g., hard drives) and media (e.g., backup tapes); if the stored evidence can no longer be read, it has lost its value.

## 4. References

Footnote	Reference
1	California Senate Bill 1386 Law on Notification of Security Breach
2-5, 30	California Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information
7	National Institute of Science and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Science and Technology
8	American National Standards Institute (ANSI) / International Committee for Information Technology Standards (INCITS) 359-2004, Role Based Access Control
9	NIST SP 800-53, Recommended Security Controls for Federal Information Systems
10	Information Systems Audit and Control Association, Information Systems Auditing Guideline: Privacy
11	NIST Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
12	ISO/IEC 17799:2000, Information Technology – Code of Practice for Information Security Management
13	NIST FIPS 197, Advanced Encryption Standard
14	Secure Identity Services Accreditation Corporation ( <a href="http://www.sisac.org">www.sisac.org</a> )
15	BITS Consumer Confidence Toolkit: Data Security and Financial Services
16	BITS Critical Success Factors for Security Awareness and Training Programs
17	Software Engineering Institute (SEI) Capability Maturity Model for Software (SW-CMM)
18	BITS Framework for Managing Technology Risk for IT Service Provider Relationships
19	CIO Executive Council, Eight Best Practices for Disaster Recovery
20	Internet Engineering Task Force (IETF) Request for Comment (RFC) 3280, Internet Public Key Infrastructure (PKI) X.509 Certificate and Certificate Revocation List Profiles
21	Security Assertion Markup Language (SAML)
22	Liberty Alliance
23	Web Services Security (WS-Security)
24	Shibboleth Project
25	IETF RFC 2246, Transport Layer Security (TLS)
26	IETF RFC 2401, Security Architecture for the Internet Protocol
27	IETF RFC 2633, S/MIME Version 3.0 Message Specification
27	IETF RFC 3851, S/MIME Version 3.1 Message Specification
28	IETF RFC 2440-bis15, Internet Draft, OpenPGP Message Format
29	Secure Identity Services Accreditation Corporation (SISAC), Certificate Policy Requirements Document (CPRD) v1.4

Footnote	Reference
31	NIST SP 800-61, Computer Security Incident Handling Guide
N/A	Public Interest Research Groups (PIRG) are a network of independent, state-based, citizen-funded organizations that advocate for the public interest. ( <a href="http://www.pirg.org/">http://www.pirg.org/</a> )
N/A	The National Conference of State Legislatures (NCSL) is a bipartisan organization that serves the legislators and staffs of the nation's 50 states, its commonwealths and territories. ( <a href="http://www.ncsl.org/">http://www.ncsl.org/</a> )
N/A	The Consumer Data Industry Association is an international trade association that represents consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services. ( <a href="http://www.cdiaonline.org">www.cdiaonline.org</a> )
N/A	Consumers Union, <a href="#">publisher of Consumer Reports</a> , is an independent, nonprofit testing and information organization serving only consumers <a href="http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf">http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf</a>

## Exhibit A

### State Legislation Data Element Matrix

State	Bill No.	Effective Date	DATA POINTS / STATE	Encrypted	Confidentiality or Integrity	Computerized Only	All media	Name, Initials	SSN	Driv Lic# or Personal and/or State ID #	Any Fin Acct# (chking acct, sav acct, credit card, debit card, pin/pw)	DOB	Mother Maiden Name or Parent's Surname	Electronic, or Digital Signatures	Biometric Data	Fingerprints	Medical Information	Employment Info
AR	SB 1167	8/12/05	8	X	X	X		X	X	X	X						X	
CA	SB 1386	7/1/03	7	X	X	X		X	X	X	X							
CT	SB 650	1/1/06	6	X		X		X	X	X	X							
DE	HB 116	6/28/05	8	X	X	X		X	X	X	X						X	
FL	HB 481	7/1/05	7	X	X	X		X	X	X	X							
GA	SB 230*	6/6/05	7	X	X	X		X	X	X	X							
IL	HB 1633	1/1/06	7	X	X	X		X	X	X	X							
IN	Act 503*	6/30/06	7	X	X	X		X	X	X	X							
LA	SB 205	1/1/06	7	X	X	X		X	X	X	X							
ME	LD 1671	1/31/06	7	X	X	X		X	X	X	X							
MN	HF 2121*	1/1/06	7	X	X	X		X	X	X	X							
MT	HB 732	3/1/06	7	X	X	X		X	X	X	X							

NJ	AB4001	1/1/06	7	X	X	X		X	X	X	X							
NY	AB4254	1/18/06	7	X	X	X		X	X	X	X							
NV	SB 347	1/1/06	7	X	X	X		X	X	X	X							
NC	SB 1048	12/1/05	9	X			X	X	X	X	X			X	X	X		
ND	SB 2251	7/1/05	10	X		X		X	X	X	X	X	X	X				X
RI	H 6191	3/1/06	7	X	X	X		X	X	X	X							
TN	SB 2220	7/1/05	7	X	X	X		X	X	X	X							
TX	SB 122	9/1/05	7	X	X	X		X	X	X	X							
WA	SB6043	7/24/05	7	X	X	X		X	X	X	X							
				21	18	20	1	21	21	21	21	1	1	2	1	1	2	1

- GA SB 251 Only information brokers are required to notify breach.
- IN SB 503 Applicable to only State agencies
- MN HF 2121 Exclude Financial and HIPPA entities