

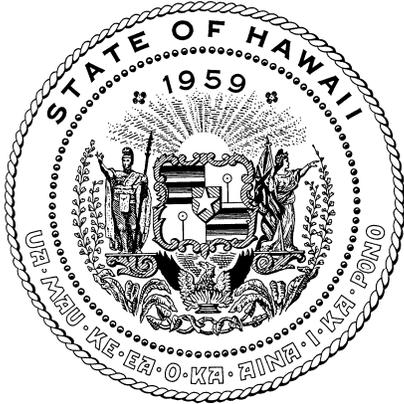
HAWAI'I IDENTITY THEFT TASK FORCE REPORT

A Report to the
Governor and the
Legislature of the
State of Hawai'i

Hawai'i Identity Theft
Study
Prepared by
J.W. Loo & Associates

December 2007

THE AUDITOR
STATE OF HAWAI'I



HAWAI'I IDENTITY THEFT TASK FORCE REPORT

A Report to the
Governor and the
Legislature of the
State of Hawai'i

Hawai'i Identity Theft
Study
Prepared by
J.W. Loo & Associates

December 2007

THE AUDITOR
STATE OF HAWAI'I

This page intentionally left blank

Introduction

In 2005, the Legislature addressed the growth of identity theft by physical means, phishing and other forms of electronic commerce crimes by creating the Hawai‘i Anti-Phishing Task Force to develop state policy on combating such crimes. As a result of the work of that task force, criminal identity theft laws were strengthened and laws protecting the security of personally identifiable information were enacted. In 2006, the Legislature (through Act 140, Session Laws of Hawai‘i 2006) continued the task force, but recognizing the broader scope of electronic crimes, reconstituted the task force as the Hawai‘i Identity Theft Task Force (“Task Force”) and increased its membership to allow for representation from more segments of the community. The Task Force’s responsibility was to address primarily personal information collected and maintained by state and county government. The Task Force was charged with:

- (a) Identifying best practices to prevent identity theft relating to personal identifying information collected by government agencies;
- (b) Establishing a timetable for the removal of personal identifying information from public records in Hawai‘i;
- (c) Reviewing current practices associated with use and disclosure of Social Security numbers;
- (d) Reviewing the current volume of records and the likely future growth in volume;
- (e) Determining the practicality of mandatory redaction of certain types of records; and
- (f) Identifying and recommending solutions for Social Security number protection.

The twenty-three member Task Force met from 2006 through 2007. Some members were identified in Act 140 and others were appointed by the President of the Senate, Speaker of the House, county prosecutors, county police chiefs, and county mayors. The members are:

Task Force Member	Appointing Authority
Gary Caulfield, Chair Vice Chairman, First Hawaiian Bank	House Speaker, Financial Services Industry
Marvin Dang, Vice Chair Hawai‘i Financial Services Association	Senate President, Financial Services Industry
Clayton Arinaga, Assistant Chief, Kaua‘i Police Department	County Police Departments
Lt. Andrew Castro Criminal Investigation Division, Financial Fraud Detail	Honolulu Police Department
Craig A. DeCosta, Prosecuting Attorney, County of Kaua‘i	Hawai‘i Prosecuting Attorneys Association

Task Force Member	Appointing Authority
Senator Carol Fukunaga	Senate President
Faye Ikei, Acting Assistant Superintendent, succeeded Darwin Ching, Member, Board of Education	Department of Education
Jodi Ito, Information Security Officer , succeeded David Lassner, Chief Information Officer	University of Hawai‘i
See note below.	U.S. Attorney
Representative Jon Riki Karamatsu	House Speaker
Nathan Kim, Department Chief, Support Services Department	Administrative Director of the Judiciary
Paul Kosasa, CEO, ABC Stores	House Speaker, Retail and Small Business
Stephen H. Levins, Executive Director	Office of Consumer Protection
Tim Lyons, President, The Legislative Center	House Speaker, Consumer and Business Organizations
Senator Ron Menor	Senate President
Representative Colleen Meyer	House Speaker
Carol Pregill, President, Retail Merchants Hawai‘i	Senate President, Retail and Small Business Community
Mel Rapozo, President	Hawai‘i Association of Counties
Robert Takushi	Senate President, Consumer and Business Organizations
Tom Terry, Supervisor / Postal Inspector	U.S. Postal Service
Rick Walkinshaw, Assistant to the Special Agent in Charge	U.S. Secret Service
Sharon Wong, Branch Manager, Planning and Project Management Office, ICSD	Department of Accounting and General Services
Christopher D.W. Young, Deputy Attorney General	Department of the Attorney General

Note: Act 140 appointed the U.S. Attorney or a representative to the task force. Due to Department of Justice policies restricting participation in the legislative process, the U.S. Attorney was not able to participate. However, Assistant U.S. Attorney Ronald Johnson was available for consultation by the task force.

Act 140 designated the Office of the Auditor to provide research and organizational support to the Task Force. The main body of this report was prepared by J.W. Loo & Associates, the consultant retained by the State Auditor, and reports on its research and findings and twelve recommendations adopted by the Task Force.

Through a survey of all state and county agencies and presentations by select agencies, the Task Force constructed a snapshot of personal information collected and maintained by agencies and the safeguards in place.

- Types of records range from human resources records of government employees and retirees to records necessary to provide services (e.g. elections, health, housing, human services, labor, utilities, land and natural resources management), to legal and regulatory records (e.g. professional licenses, law enforcement, court proceedings, and tax administration).
- State and county agencies maintain between 20 and 30 million records containing personal information. Fifteen of the eighty-five agencies surveyed reported over one million records; ten of the fifteen estimate annual growth of 6% - 10%.
- There is an absence of comprehensive administrative, technical, and physical safeguards covering privacy and security of personal information at state and county agencies.
 - Training on handling and security of personal information records often is, at best, informal. Only one-fourth of the agencies surveyed reported mandatory employee training on the appropriate use and disclosure of personal information.
- Some agencies collect personal information, such as Social Security numbers, without an apparent business purpose.
- Nearly all of the agencies surveyed reported transmitting information outside of the organization. Just over one-half have specific procedures for concealing or redacting personal information on paper documents, and less than one-half reported technical safeguards in place for electronic transmission of information or storage of personal information on laptop computers or removable storage devices.

The Task Force recognizes that some solutions will require more time and funds. However the Task Force chose to focus on more immediate concerns and solutions that will have an immediate impact on security of personal information. The Task Force believes agencies must act, with a sense of urgency, to secure their records, to institute basic security policies, and to reduce collection of personal information to only that which is necessary. An agency that collects and

maintains personal information must accept that the use of this information comes with a responsibility to safeguard, not as an afterthought, but as a priority.

The Task Force recommendations will limit the exposure of personal information and can be implemented by state and county agencies immediately and at minimal cost, however the Task Force believes responsibility must start at the highest level of government. There must be a commitment to security, otherwise a comprehensive policy will not be possible and personal identifying information will be exposed to a substantial risk of loss. Therefore, one of the recommendations is the formation of an Information Privacy and Security Workgroup, appointed by the Governor, to develop guidance and best practices to be made available to all agencies.

The Task Force also reviewed recommendations for victims of identity theft, law enforcement, and the private sector. For victims of identity theft, the Task Force recommends the Information Privacy and Security Workgroup submit to the Legislature an assessment and recommendations on initiatives to mitigate the impact of identity theft incidents on individuals.

Law enforcement representatives on the Task Force reported that changes to the criminal definition of identity theft recommended by the Hawai'i Anti-Phishing Task Force and enacted in 2006 have been very effective and should be allowed to continue without change.

Private sector representatives recommended the Task Force develop a flyer describing the identity theft laws and where businesses may find information. Appendix 5 is a sample flyer that may be disseminated to businesses.

The Task Force's twelve recommendations, briefly summarized here, fall under four broad categories and are discussed in detail in the report:

Summary of Hawai'i Identity Theft Task Force Recommendations

Decrease unnecessary use of personal information

Recommendation 1: Require annual report on systems that use personal information

Recommendation 2: Limit the personal information in agency records

Recommendation 3: Reduce the use of social security numbers

Implement safeguards to protect personal information

Recommendation 4: Require state and county agencies to assign policy and oversight responsibilities

Recommendation 5: Issue guidance on use of personal information in human resources functions

Recommendation 6: Require state and county agencies to use third party information use agreements

Ensure effective, risk-based responses to data breaches

Recommendation 7: Issue data breach guidance to agencies

Recommendation 8: Require agencies to develop and implement a breach notification policy

Recommendation 9: Assess and recommend to the Legislature initiatives to mitigate the impact of identity theft on individuals

Educate agencies on how to protect data

Recommendation 10: Develop concrete guidance and best practices

Recommendation 11: Issue portable storage and communication devices guidance to agencies

Revise the Effective Date of Required Social Security Number Protection Measures

Recommendation 12: Revise the effective date of the Social Security Protection law, HRS Chapter 487J, to July 1, 2009

Protecting and safeguarding personal information is critical to preventing identity theft crimes. The Task Force has learned that state and county agencies have much to do to prevent loss of personal information in records they maintain. We respectfully ask the State and County administrations and the State Legislature to seriously consider and act on the Task Force recommendations.

Foreword

The 2006 Legislature, through Act 140, Session Laws of Hawai‘i 2006, created the Hawai‘i Identity Theft Task Force as the successor to the Anti-Phishing Task Force which was created in 2005. Charged with identifying best practices to prevent identity theft and protecting personal identifying information collected by government agencies, the Task Force submits its findings and recommendations in this report.

On behalf of the Hawai‘i Identity Theft Task Force as well as my office, we wish to express our appreciation for the cooperation and help of the many individuals who contributed to this report. We also want to thank our consultant, J.W. Loo and Associates, for its assistance and commitment to this project.

Marion M. Higa
State Auditor

This page intentionally left blank

Chair's Message

Aloha,

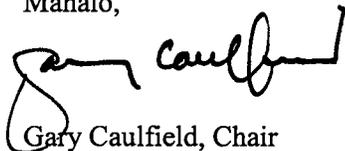
When the Hawai'i Identity Theft Task Force convened in September 2006, there were daily media reports of breaches and identity theft incidents across the country. Nearly half of the breaches in 2006 and 2007 involved universities and state and local governments. The Legislature's direction to the Task Force was to examine the availability of personal information in government, current government practices in Hawaii, trends and practices in other states, and to make recommendations to protect the personal information in state and county government records. We surveyed all of the agencies and listened to a number of presentations by state and county agencies, and we came to understand that there was a large and growing volume of records, and most agencies lacked administrative and technical safeguards over those records.

Our goal was to develop recommendations that could be implemented in a short time frame and which would provide government agencies with a direction, framework and tools needed to move forward in securing personal information. We believe we have succeeded. Once adopted, the Task Force's recommendations would reduce the amount of personal information used and require agencies to implement safeguards and effective responses to data breaches and educate employees on protecting data.

We are pleased to present the report of the Hawai'i Identity Theft Task Force and twelve recommendations to improve the security of personal information collected and maintained by government agencies. We urge the Legislature and State and County administrations to act on these recommendations, as they will have an impact in protecting Hawai'i residents from identity theft.

Thank you to the twenty-two other members of the Task Force for their contributions and time, to the private sector organizations that contributed to this report, to the consultant, J.W. Loo and Associates, and to the Office of the Auditor for their support.

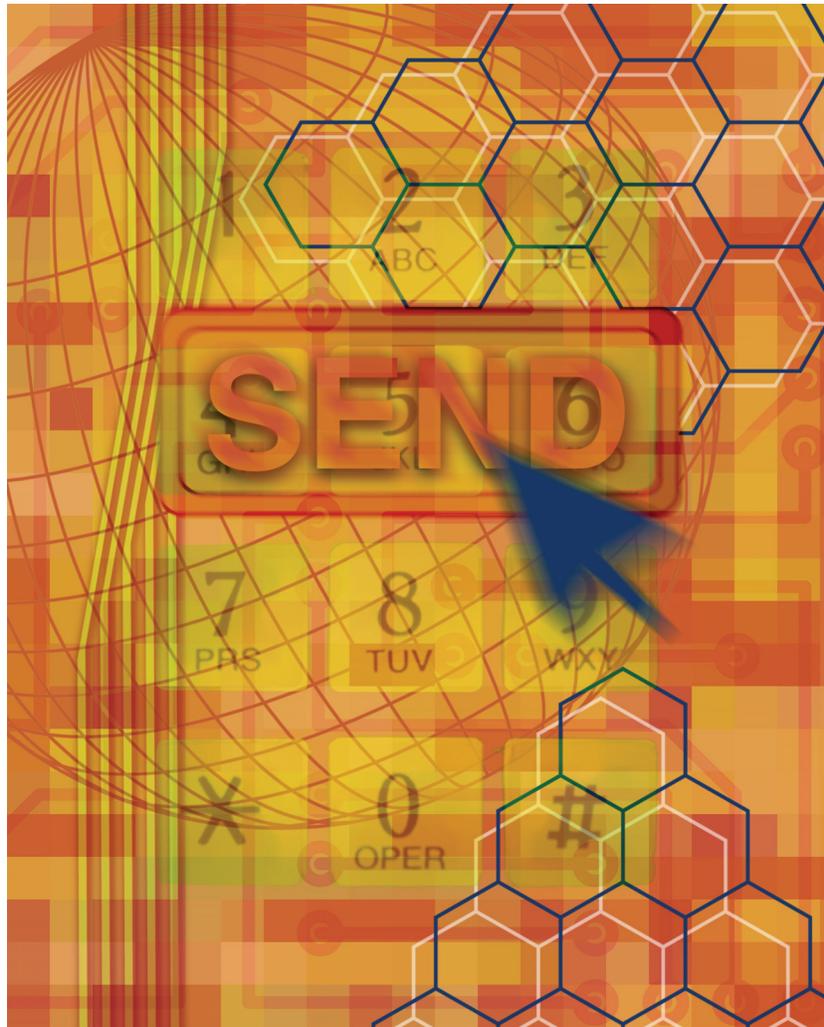
Mahalo,



Gary Caulfield, Chair
Hawai'i Identity Theft Task Force

This page intentionally left blank

IDENTITY THEFT TASK FORCE STUDY: PERSONAL INFORMATION IN HAWAI`I GOVERNMENT AGENCIES



Prepared for
**The State of Hawai`i
Identity Theft Task Force**

Prepared by
J.W. LOO AND ASSOCIATES

December 2007

This page intentionally left blank

Table of Contents

SECTION 1. OVERVIEW	4
Background	4
Methodology	4
SECTION 2. DEFINE PERSONAL INFORMATION	7
Hawai'i Statutes	7
Identity Theft	7
Security Breaches	7
Destruction of Personal Information Records	8
Other State Jurisdictions Statutes	8
Identity Theft	8
Security Breaches	13
SECTION 3. AGENCY PERSONAL INFORMATION PRACTICES	14
Personal Information in Government Records	14
Social Security Number Use/Disclosures	14
Volume and Annual Volume Growth of Government Records	18
Records Volume	18
Records Volume Growth	20
SECTION 4. BEST PRACTICES TO PREVENT IDENTITY THEFT	22
President's Task Force on Identity Theft Strategic Plan	22
State Laws and Initiatives	23
Assign Policy and Oversight Responsibilities	23
Decrease the Unnecessary Use of SSN	26
Reduce Information Technology Security Risks to an Acceptable Level	29
Establish a Comprehensive Framework for Ensuring the Effectiveness of Information Security Controls Over Information Resources	30
Require Agencies to Prepare Extensive Data Collection Analyses and Report Periodically to the Responsible Executive and Legislative Branch Oversight Units	32
Implement Agency Training on Security Awareness Topics and on How to Respond to Data Breaches	32
Mitigate the Impact of Security Breaches	34
SECTION 5. RISK ASSESSMENT AND FINDINGS	37
Personal Information Collected by Agencies	37

Volume and Growth of Records	38
Patterns of Use and Disclosures	39
Personal Information Disclosure Means	44
Physical and Technical Safeguards Deployed by Agencies	45
Business Associate Agreements	47
Administrative Safeguards	47
SECTION 6. IDENTITY THEFT TASK FORCE RECOMMENDATIONS	50
Decrease Unnecessary Use of Personal Information	50
Recommendation No. 1. Require Annual Report on Systems that Use Personal Information	50
Recommendation No. 2. Limit the Personal Information in Agency Records	50
Recommendation No. 3. Reduce Use of Social Security Numbers	51
Implement Safeguards to Protect Personal Information	51
Recommendation No. 4. Require State and County Agencies to Assign Policy and Oversight Responsibilities	52
Recommendation No. 5. Issue Guidance on Use of Personal Information in Human Resources Functions	52
Recommendation No. 6. Require State and County Agencies to Use Third Party Information Use Agreements	53
Ensure Effective, Risk-Based Responses to Data Breaches	53
Recommendation No. 7. Issue Data Breach Guidance to Agencies	53
Recommendation No. 8. Require Agencies to Develop and Implement a Breach Notification Policy	54
Recommendation No. 9. Assess and Recommend Initiatives to Mitigate the Impact of Identity Theft on Individuals	54
Educate Agencies on How to Protect Data	55
Recommendation No. 10. Develop Concrete Guidance and Best Practices	55
Recommendation No. 11. Issue Portable Storage and Communication Devices Guidance to Agencies	55
Revise the Effective Date of Required Social Security Number Protection Measures	55
APPENDIX 1. PERSONAL INFORMATION DEFINITIONS	57
APPENDIX 2. PERSONAL INFORMATION IN GOVERNMENT RECORDS	80
APPENDIX 3. VOLUME OF GOVERNMENT RECORDS CONTAINING PERSONAL INFORMATION	84
APPENDIX 4. BEST PRACTICES IN OTHER STATE JURISDICTIONS	90
APPENDIX 5. BROCHURE FOR BUSINESSES	141

APPENDIX 6. SUMMARY OF STATE AND COUNTY AGENCIES PRESENTATIONS TO THE HAWAI'I ID THEFT TASK FORCE	145
EXHIBIT 1. PERSONAL INFORMATION QUESTIONNAIRE	154
EXHIBIT 2. CALIFORNIA BUSINESS AND PROFESSIONS CODE, SECTION 350-352	165
EXHIBIT 3. MISSOURI REVISED STATUTES, CHAPTER 59, COUNTY RECORDERS OF DEEDS, SECTION 59.331 AUGUST 28, 2007	166
EXHIBIT 4. CALIFORNIA CODES, CIVIL CODE SECTION 1798-1798.1	167
EXHIBIT 5. CALIFORNIA CODES, CIVIL CODE SECTION 1788.18	181

Section 1. Overview

Background

The Identity Theft Task Force is a continuation of the Anti-Phishing Task Force, created by the 2005 Legislature, but with added members and responsibilities. Act 140 (2006 Session Laws) changed the name of the Anti-Phishing Task Force to the Identity Theft Task Force (Task Force), added twelve members, and moved administrative responsibility from the Office of the Attorney General to the Office of the Auditor. In addition, new provisions assigned the Task Force responsibility to:

1. Identify best practices related to protecting personal identifying information collected by government agencies.
2. Review other jurisdictions' activities, policies, and laws.
3. Establish a timetable for removal of personal identifying information from public records.
4. Review current practices in the use and disclosure of Social Security numbers in state and county records and documents.
5. Review the volume of these records and documents and likely future increase or decrease.
6. Review the impact of mandatory redaction.
7. Identify and recommend solutions for protecting Social Security numbers.

The Task Force is to report its findings and recommendations to the Legislature prior to the convening of the 2007 and 2008 regular sessions. A final report which will include the Task Force's findings and recommendations is to be submitted prior to the 2008 regular session.

Methodology

The Task Force work was divided into two (2) phases. In Phase One, the following tasks were performed:

1. Define personal identifying information
2. Perform a risk assessment of state and county agencies based on volume of personal identifying information collected and maintained and the risk and impact of disclosure.
3. Identify best practices to prevent identity theft by reviewing other jurisdictions' activities, policies, and laws related to protecting personal information collected by government agencies.
4. Review current practice in the use and disclosure for public inspection of social security numbers (SSN) in records and documents maintained by Hawai'i state and county agencies.

For Phase Two, the following tasks were performed:

1. Review the current volume of documents and records containing personal identifying information and assess the future growth or decline in volume.
2. Examine the practicability of mandatory redaction and the impact of implementation on human and other resources.
3. Propose a timetable for the immediate removal of personal identifying information from public records in Hawai`i.
4. Identify and recommend solutions to issues related to protection of SSNs, including the sale, lease, trade, rent, or otherwise intentional release of an individual's SSN to a third party.

To address the assigned task areas, a general literature search was initiated to identify baseline facts and prospective information sources. In addition to media sources and news clips, research reports from leading industry resources including the United States General Accounting Office¹, Javelin Strategy & Research², McAfee³, The National Archives (UK)⁴, and Symantec⁵ were compiled and reviewed.

For the *define personal identifying information* task, statutes for all fifty (50) states were searched for references to *personal identifying information* and close term of reference variations. Emphasis was placed on terms associated with identity theft and security breach provisions. The statutory definitions were then compiled and analyzed to identify variations in definition constructs and content.

For the *identify best practices to prevent identity theft* task, the websites of all fifty (50) states were searched to identify website links, statutes, press releases, education materials, study documents, and activity descriptions pertinent to identity theft prevention initiatives in the respective states. Specific emphasis was placed on identifying the following information:

1. Assigned responsibilities for identity theft related roles and tasks.
2. Laws and activities to reduce government exposure to identity theft and security breach incidents.
3. Laws and activities targeting identity theft prevention and measures to mitigate the impact to individuals of identity theft/security breach incidents
4. Laws and activities to educate government agencies and staff on identity theft/security breach topics
5. Laws and activities to implement safeguards to protect personal information managed by government agencies.

¹ United States General Accounting Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, June 2007

² Javelin Strategy & Research, 2006 Identity Fraud Survey Report, January 2006.

³ Francois Paget, McAfee Avert Labs White Paper, *Identity Theft*, January 2007.

⁴ The National Archive, *Redaction: Guidelines for the Editing of Exempt Information from Paper and Electronic Documents Prior to Release*, March 2006

⁵ Symantec, *Symantec Internet Security Threat Report: Trends for July-December 06*, Volume XI, March 2007

For the review current practice in the use and disclosure for public inspection of social security numbers (SSN) in records and documents and review the current volume of documents and records containing personal identifying information tasks, a survey of State and County agencies was performed. A sample of the survey is provided in *Exhibit 1, Personal Information Questionnaire*.

Survey results were reviewed to determine the scope of personal information, including SSN, used/disclosed by agencies; patterns of personal information exchange within/between departments and third parties; and modes of personal information transmittal used by agencies. They were also used to assess the risk of state and county agencies based on volume of personal information.

Section 2. Define Personal Information

Two (2) perspectives are offered on defining the term *personal identifying information*. One, there are the definitions of related terms provided in the Hawai'i Revised Statutes. And two, there are the references found in the statutes of other state jurisdictions.

Hawai'i Statutes

Relative to identity theft, there are several significant contexts found in the Hawai'i Revised Statutes (HRS) for the term *personal information*. One, the reference serves as a foundational component for defining the offense of identity theft. Two, it provides a threshold for triggering mandatory notifications to individuals in instances of information security breaches. And three, it serves as the domain of records that businesses and agencies are required to provide specified protections during destruction processes.

Identity Theft

As defined in HRS §708-800 and as it applies to the commission of identity theft in the first degree (HRS §708-839.6), identity theft in the second degree (HRS §708-839.7) and identity theft in the third degree (HRS §708-839.8), *personal information* means:

Information associated with an actual person or a fictitious person that is a name, an address, a telephone number, an electronic mail address, a driver's license number, a social security number, an employer, a place of employment, information related to employment, an employee identification number, a mother's maiden name, an identifying number of a depository account, a bank account number, a password used for accessing information, or any other name, number, or code that is used, alone or in conjunction with other information, to confirm the identity of an actual or a fictitious person.

In this usage, *personal information* encompasses a fairly expansive range of identification information types associated with persons that may be used in the commission of identity theft. It includes specifically named personal identification, employment, and financial accounts information. And it also includes other undefined information types that may be used to confirm the identity of a person.

Security Breaches

As defined in HRS §487N-1 and as it applies to required notifications to individuals in the event of security breaches (HRS §487N-2), *personal information* means:

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 Hawai'i identification card number; or*
- 3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.*

In this usage, the term *personal information* is restricted to an individual's name, specified financial identifiers, and defined information types that may be used to access an individual's

financial account(s). It excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records.

As applied to security breaches, notification to individuals would be required:

1. If the exposed *personal information* meets the definition criteria specified in HRS §487N-1.
2. If the exposed *personal information* is unencrypted.
3. And if it can be determined that there has been illegal use of the *personal information* or is reasonably likely to occur and that creates a risk of harm to a person.

Destruction of Personal Information Records

As defined in HRS §487R-1 and as it applies to required protections during processes involving personal information record disposal (HRS §487R-2), *personal information* means:

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 Hawai'i identification card number; or*
3. *Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.*

Personal information records that conform to the statutory definition in HRS §487R-1, shall be protected against unauthorized access to or use of the information in connection with or after its disposal. In this context, *personal information* is said not to include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The definitions used for personal information in the security breach (HRS §487N-1) and destruction of personal information records (HRS §487R-1) contexts are identical.

Other State Jurisdictions Statutes

Appendix 1, Personal Information Definitions, provides a compilation of personal information terms and definitions used by states in statutes relating to identity theft and security breach notifications.

As of 2007, all of the fifty (50) states have established statutes that address an identity theft crime classification associated with the illegal use of personal information. The terms of reference used display a wide range in scope and definition content.

Twenty five (25) of the states have established statutes relating to required notifications in events of security breaches involving personal information. Significantly, the terms of reference used in these contexts are fairly consistent and similar in definition.

Identity Theft

With respect to identity theft, the states have adopted ten (10) different terms for personal information. A summary of these terms is provided in *Personal Information – Terms of Reference, Table 1*.

Personal identifying information is the most common as it is used by twenty seven (27) of the states. Next in use frequency are the terms *identifying information*, *personal information*, and *identifying information*.

	Term Used	States
1	Identifying Information	Alabama, Pennsylvania, South Carolina, South Dakota, Virginia
2	Personal Information	Alaska, Hawai'i, Oklahoma, West Virginia
3	Personal Identifying Information	Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Idaho, Illinois, Louisiana, Maryland, Massachusetts, Michigan, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Dakota, Ohio, Tennessee, Texas, Utah, Vermont, Wisconsin, Wyoming
4	Personal Identification Information	Florida, Oregon
5	Identifying Information	Georgia, Indiana, Kentucky, North Carolina
6	Identification Information	Iowa
7	Identification Document	Kansas
8	Legal Identification	Maine
9	Identity	Minnesota
10	Means of Identification	Missouri, Rhode Island, Washington

Personal Information – Terms of Reference,
Table 1

Use of the same term of reference does not appear to suggest uniformity in definition. In fact, there are instances where there is much similarity in definitions among states that use different terms of reference and conversely, significant differences among states using similar terms.

As an example, both District of Columbia and Colorado use the term *personal identifying information*. The definition used by the District of Columbia⁶ is:

Includes, but is not limited to, the following:

(A) Name, address, telephone number, date of birth, or mother's maiden name.

(B) Driver's license or driver's license number or non-driver's license or non-driver's license number;

(C) Savings, checking or other financial account number;

(D) Social security number or tax identification number;

⁶ D.C Code 22-3227.01

- (E) Passport or passport number;*
- (F) Citizenship status, visa, or alien registration card or number;*
- (G) Birth certificate or a facsimile of a birth certificate*
- (H) Credit or debit card, or credit or debit card number*
- (I) Credit history or credit rating*
- (J) Signature;*
- (K) Personal identification number, electronic identification number, password, access code or device, electronic address, electronic identification number, routing information or code, digital signature, or telecommunication identifying information;*
- (L) Biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;*
- (M) Place of employment, employment history, or employee identification number; and*
- (N) Any other numbers or information that can be used to access a person's financial resources, access medical information, obtain identification, act as identification, or obtain property.*

For Colorado⁷, the definition used is:

Means information that may be used, alone or in conjunction with any other information, to identify a specific individual, including but not limited to a name; a date of birth; a social security number; a password; a pass code; an official, government-issued driver's license or identification card number; a government passport number; biometric data; or an employer, student, or military identification number.

Colorado includes references to a fairly short list of specific identification elements and suggests that other elements may also be included if they can be used to identify a specific individual. It covers information that an individual might create as well as identification information that might be generated from employers, schools or the military.

In comparison, the District of Columbia uses a similar definition structure but includes a substantially larger scope of specified identifiers. Besides individual identifiers, the District of Columbia also includes information that can be used to construe the identity of an individual (e.g. address, telephone number, birth certificate), financial accounts information, information that can be used to access an individual's financial account (e.g. passwords, biometric data), and telecommunication identifying information. And the District of Columbia also includes identifiers that can be used to access an individual's medical information in its definition.

⁷ Colorado Revised Statutes Section 18-5-901

With respect to definition constructs, the states have created definitions that range from the general to specific, itemized list structures. For instance, Alaska⁸ uses a definition of *personal information* that includes:

Information that can be used to identify a person and from which judgments can be made about a person's character, habits, avocations, finances, occupation, general reputation, credit, health, or other personal characteristics, but does not include a person's name, address, or telephone number, if the number is published in a current telephone directory, or information describing a public job held by a person.

Alaska's use of the generalized form is a clear attempt to include a wide range of information types that may be illegally used in identity theft without creating an itemized listing that may omit uncommon and/or newly appearing identifiers or information that could be used to construe an individual's identity.

In contrast, Arizona⁹ uses a definition structure that is expansive and specific. Arizona defines *personal identifying information* as meaning:

Any written document or electronic data that does or purports to provide information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number, photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information.

Recognition of and emphasis on electronic and/or biometric identifiers varies among the states. Some states such as California¹⁰ make specific reference to these identifier types including *unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device.*

Other states such as Idaho¹¹, *Personal identifying information*:

Means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, checking account number, savings account number, financial transaction card number, or personal identification code of an individual person, or any other numbers or information which can be used to access a person's financial resources.

⁸ Alaska Statutes Section 40.25.350(2)

⁹ Arizona Revised Statutes Section 13-2001

¹⁰ California Code Section 530.55

¹¹ Idaho Code Section 18-3122

and Kansas¹², *Identification document*:

Means any card, certificate or document or banking instrument including, but not limited to, credit or debit card, which identifies or purports to identify the bearer of such document, whether or not intended for use as identification, and includes, but is not limited to, documents purporting to be drivers' licenses, nondrivers' identification cards, certified copies of birth, death, marriage and divorce certificates, social security cards and employee identification cards.

make no specific reference to electronic or biometric identifiers at all.

Other notable attributes found in the statutory definitions used by the states include:

1. Arizona¹³ includes a reference to electronic identifier or screen name in its definition of *personal identifying information*. It also includes the image of an iris or deoxyribonucleic acid or genetic information.
2. Arkansas¹⁴ includes digital signature in its itemization of identifying information.
3. California¹⁵ includes address or routing code and telecommunication identifying information or access device.
4. Delaware¹⁶ includes e-mail address and computer system password.
5. District of Columbia¹⁷ includes credit history or credit rating and place of employment or employment history.
6. Florida¹⁸ includes Medicaid or food stamp account number and medical records.
7. Georgia¹⁹ cites current or former names.
8. Illinois²⁰ includes digital signals.
9. Indiana²¹ includes telecommunication access device, including a card, a plate, a code, a telephone number, an account number, a personal identification number, an electronic serial number, a mobile identification number, or another telecommunications service or device or means of account access that may be used to obtain money, goods, services, or any other thing of value or initiate a transfer of funds.
10. Iowa²² includes logo, symbol, and trademark.
11. Nevada²³ includes the number, code or other identifying information of a person who receives medical treatment as part of a confidential clinical trial or study, who participates in a confidential clinical trial or study involving the use of prescription drugs or who participates in any other confidential medical, psychological or behavioral experiment, study or trial.

¹² Kansas Statutes Section 21-3830

¹³ Arizona Revised Statutes Section 13-2001

¹⁴ Arkansas Code Section 5-37-227

¹⁵ California Code Section 18-5-901

¹⁶ Delaware Code Section 854

¹⁷ D.C. Code 22-3227.01

¹⁸ Florida Statutes Section 817.568

¹⁹ Georgia Code Section 16-9-120

²⁰ 720 Illinois Compiled Statutes 5/16G

²¹ Indiana Code 35-43-5-1

²² Iowa Code 715A.8

²³ Nevada Revised Statutes 205.4617

12. North Carolina²⁴ includes electronic identification numbers, electronic mail names, or addresses, Internet account numbers, or Internet identification names.
13. Oregon²⁵ includes a person's photograph.
14. Vermont²⁶ includes identification document or false identification document.

Security Breaches

Of the twenty five (25) states that have established statutes relating to required notifications in events of security breaches involving personal information, all except Texas use *personal information* as the term of reference. Texas uses the term *sensitive personal information*.

All of the states use a similar definition construct that follows the general structure:

1. Individual's name (first name, initial and/or last name)
2. Individual's social security number
3. Individual's driver or other identification number
4. Individual's financial account numbers with any required security code that would permit access to the individual's financial account

Most of the states stipulate that notification to individuals is mandated when an individual's name in combination with one of the three specified personal information identifiers is exposed to unauthorized access. For some states, a qualifier is that there must be determined to be illegal use or the likelihood of harm to an individual. An additional qualifier for some states is that the personal information is unsecured and/or unencrypted.

There is some variation among the states regarding account information that is specified. Among these are:

1. Arkansas²⁷ includes medical information.
2. Nebraska²⁸ includes unique electronic identification number or routing code, in combination with any required security code, access code, or password; unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation

²⁴ North Carolina General Statutes Section 14-113.20)

²⁵ Oregon Revised Statutes Section 165.800

²⁶ Vermont Statutes Section 2030

²⁷ Arkansas Code Section 4-110-103

²⁸ Nebraska Revised Statutes Section 87-802

Section 3. Agency Personal Information Practices

Personal Information in Government Records

According to responses to the personal information questionnaire distributed to Hawai'i state and county agencies in January 2007, personal information is *handled, processed, or stored* in a broad range of document/record types to support government processes spanning government operations, services to the public, services to businesses/industries, and legal/regulatory compliance. A summary of record types reported by agencies containing personal information is provided in *Appendix 2 Personal Information in Government Records*.

Personal information in records supporting government human resource management processes is reportedly used/disclosed in a majority of Hawai'i agencies. Records containing personal information related to procurement management processes are also reported to be commonly used/disclosed in many of the Hawai'i agencies.

Relating to services to the public, personal information is reported used/disclosed in support of functions performed by respective executive branch agencies ranging from elections, health, housing, human services, labor, utilities, and land/natural resources management. In these contexts, the subjects of personal information include voter registrants, newborns, decedents, marriage/divorce applicants, emergency services recipients, individuals receiving vaccinations, individuals in foster homes, individuals receiving adult protective services, individuals receiving child welfare services, rental housing applicants and tenants, social services and welfare recipients, foster parents, individuals with wage complaints, child labor applicants, individuals with discrimination complaints, workers' compensation claimants, individuals with temporary disability insurance disputes, unemployment benefits claimants, job training applicants/participants, employment/apprenticeship program participants, real property titleholders, land applicants/lessees, and hunting/fishing license applicants.

Personal information is also reported used/disclosed to support services to businesses/industries including business registration, trade name/trademark/service mark registration, professional licensing, and economic development loans. In these contexts, the subjects of personal information are generally individuals owning businesses where the ownership form is a sole proprietorship.

And in legal and regulatory compliance functions, personal information is reported used/disclosed in records to support processes including arrests, investigations and complaints, civil actions, probate proceedings, guardianship proceedings, probate proceedings, trust proceedings, torts, criminal actions, Family Court proceedings, tax administration, inmate supervision, parole determination, warrants, traffic reporting, emergency incidents, and crime victim compensation.

Social Security Number Use/Disclosures

In the January 2007 personal information survey, questions were posed to determine current practices in the use and disclosure for public inspection of social security numbers (SSN) in records and documents maintained by Hawai'i state and county agencies.

Agencies were specifically queried if they use/disclose records containing individual SSNs. Seventy five (75) agencies representing 85% of responding agencies answered in the affirmative. In most instances, agencies reported that the records containing SSNs were in support of human resource and/or procurement management related processes.

To determine their readiness to comply with SSN protection provisions contained in Chapter §487J (Social Security Number Protection), agencies that stated that they use/disclose SSN during the course of business were posed several follow up questions:

During the course of business, does your agency communicate or otherwise make available to the general public an individual's entire Social Security Number?

Of responding agencies, four (4) replied in the affirmative.

1. Hawai'i State Department of Health. SSNs are included in letters and discharge reports that are required by health care plans and primary care providers.
2. Hawai'i State Department of Labor and Industrial Relations. SSN information is provided to parties of interest (e.g. employer, insurance carriers, health care providers, attorneys) for case administration purposes.
3. Hawai'i State Department of Land and Natural Resources. Contractors file payroll records and tax clearances which become public records. Conveyance documents, considered public records, may include SSN information.
4. The Judiciary. SSN information may be contained in case documents and on bail receipts

During the course of business, does your agency print/embed an individual's entire Social Security Number on any card required for the individual to access services provided by the agency?

Of responding agencies, five (5) replied in the affirmative. Four (4) of the reported use/disclosure contexts appear to involve agency employees and only one (1) involves public individuals.

1. Hawai'i State Department of Education. SSNs are required in professional certification transcripts and program applications.
2. Hawai'i State Department of Health. SSNs required for statements of intra-state travel completed.
3. Hawai'i State Department of Land and Natural Resources. SSNs required to apply for hunting licenses.
4. County of Kauai, Department of Finance. The Driver License Division discloses that SSNs are required on unspecified cards/forms.
5. County of Kauai, Office of Community Assistance. The SSN or State identification card is required to obtain security access cards and key to enter county work facility.

During the course of business, does your agency require individuals to transmit the individual's entire Social Security Number to access an Internet website?

Fifteen (15) agencies answered this question in the affirmative. Notable use/disclosure contexts include:

1. Hawai'i State Department of Defense. The SSN is transmitted in Internet applications used by the Office of Veterans Services and the Youth Challenge Academy.
2. Hawai'i State Department of Education. The SSN is transmitted in the HOUSSSE Internet application used to support professional development activities.
3. Hawai'i State Department of Hawaiian Home Lands. The SSN is transmitted over the Internet to obtain credit reports for lessees.

4. Hawai'i State Department of Labor and Industrial Relations. The Office of Community Services reported that SSN information is transmitted over the Internet, secure Internet connections are not used, and SSN information is not encrypted.
5. Hawai'i State Department of Land and Natural Resources. SSN information is required for online applications for hunting and freshwater game fishing licenses. The data is transmitted via the eHawai'i.gov website using secure Internet connections.
6. Hawai'i State Department of Taxation. Taxpayers who use the state website to file tax returns and who access the website to inquire about the status of their refunds are required to enter their entire SSN. The agency stated that all electronic transmissions are handled through the state website, eHawai'i.gov using SSL connections.
7. Honolulu Office of the Mayor. The Office of Culture and the Arts reported that SSN information is transmitted over the Internet when individuals make online payment requests.
8. Honolulu Department of Community Services. Stated that SSN information is transmitted over the Internet when credit information is requested.

During the course of business, does your agency require individuals to use the individual's entire Social Security Number to access an Internet website?

Four (4) agencies responded to this question in the affirmative. One of these, the Hawai'i Department of Land and Natural Resources stated that SSN is not required to access their website but is required to complete license application forms.

1. Hawai'i State Department of Human Services. The Management Services Office reported SSN is required when reviewing cases worked on by division staff.
2. Honolulu Department of Community Services. Stated that SSN is required to access the website to obtain credit information.

During the course of business, does your agency unit print an individual's entire Social Security Number on any materials that are mailed to the individual?

Forty four (44) agencies responded affirmatively with most of the reported instances involving transmittal of human resources and/or procurement forms (e.g. Form 1099-Misc, Form W-2, EUTF form L-1) to employees or contractors. Other notable SSN disclosure contexts include:

1. Hawai'i State Department of Attorney General. Orders for Income Withholding (OIW) sent to the Child Enforcement Agency and to employers contain SSN information. Child support case documents required by federal and judicial regulations and rules contain SSN information.
2. Hawai'i State Department of Business Economic Development and Tourism. Reported that for contractors who are individuals, the SSN is printed on letters of agreement and contracts.
3. Hawai'i State Department of Defense. The Office of Veterans Service stated that SSN is required by federal Title 38 CFR.
4. Hawai'i State Department of Hawaiian Home Lands. Sales contracts and selection agreements to individuals contain SSN.
5. Hawai'i State Department of Health. The death certificate contains the entire SSN as required by the Social Security Administration. The ambulance report for individuals receiving emergency medical services will have the patient's SSN.
6. Hawai'i State Department of Human Services. The SSN is required on prescriptions and consultation packets.

7. Hawai'i State Department of Labor and Industrial Relations. The Disability Compensation Division reported that copies of claim forms and reports from parties of interest may contain SSN and may be mailed to claimants. The Unemployment Insurance Division reported that inclusion of the SSN on eligibility determination notes, request for information, and notices to report/contact the Unemployment Insurance Division is required by Section 303(f) and 1137 of the Social Security Act.
8. Hawai'i State Department of Transportation. Reported that State law requires inclusion of SSN to report tax withholding on the sale of real property owned by Hawai'i non-residents.
9. The Judiciary. In the Family Court, certain legal documents, drafted by a party, who is not represented by an attorney, may be mailed by the Court to the party.
10. Honolulu Department of Community Services. Reported that for the Family Self Support Program, certain materials have the SSN.
11. County of Kauai Department of Finance. The Driver License Division reported that for notices of license suspensions and revocations, the SSN may be used for identification and recordkeeping.

Does your agency sell, lease, trade, rent, or otherwise intentionally release individuals' SSNs to a third party?

To this question, twenty five (25) agencies, representing 17% of responding agencies, answered affirmatively. Many of the reported third party disclosures were determined to be to other government agencies. Reported instances of SSN releases to non-government entities include:

1. Hawai'i Department of Budget and Finance. Released in connections with disability cases.
2. Hawai'i Department of Commerce and Consumer Affairs. SSN information for producer licensees is released to Hawai'i Information Consortium (Hawai'i state public website vendor) and to the National Association of Insurance Commissioners.
3. Hawai'i Department of Education. Disclosed to Citistreet (deferred compensation vendor), AIG (tax shelter annuity vendor), and HGEA (union).
4. Hawai'i Department of Hawaiian Home lands. SSN is disclosed to obtain credit reports for lease applicants from the Credit Bureau of the Pacific.
5. Hawai'i State Department of Health. SSNs for deceased individuals are reported to the federal Social Security Administration. SSN for individuals who receive emergency services are reported to insurance agencies for billing purposes.
6. Hawai'i State Department of Human Resources Development. SSNs may be disclosed in response to subpoenas.
7. Hawai'i State Department of Land and Natural Resources. The Bureau of Conveyances discloses SSN information when a copy of a judgment is ordered.

8. Hawai'i State Department of Taxation. SSN information is disclosed to the Internal Revenue Service. Contractors may be provided access to SSN information but this is on a need to know basis and subject to confidentiality clauses in contract agreements.
9. Hawai'i State Department of Transportation. SSN is disclosed in relation to alcohol drug testing for commercial driver licenses.
10. Honolulu Department of Information Technology. SSN may be disclosed to ING, unions, Federal Reserve Bank.
11. Kauai Department of Public Works. SSN may be disclosed to unions and medical facilities.
12. Maui Department of Prosecuting Attorney. SSN may be disclosed to defense attorneys.

Volume and Annual Volume Growth of Government Records

Records Volume

In the January 2007 personal information questionnaire, agencies were asked to provide an estimate of the volume and of the annual volume growth of individual records containing personal information maintained by the agency. A listing of agency responses is provided in *Appendix 3, Volume of Government Records Containing Personal Information*.

A distribution table representing the volumes of agency records reported containing personal information is provided in *Table 2, Volume of Government Records Summary* below.

Volume Range	State	Honolulu	Hawai'i	Kauai	Maui	Total
1 - 100	1	4	1	2	2	10
101 – 1,000	1	4	2	4	2	13
1,001 – 10, 000	0	2	4	2	2	10
10,001 – 100,000	1	4	5	3	3	16
100,001 – 500,000	4	3	3	2	0	12
500,001 – 1,000,000	5	3	0	0	1	9
1,000,001 or more	9	3	1	0	2	15
	21	23	16	13	12	85

Volume of Government Records Summary
Table 2

In all, the volume of records maintained by state and county agencies combined is estimated to be approximately 20,000,000 – 25,000,000.

Predictably, the volume of records maintained by state agencies is substantial. In all, the total volume of records maintained by state agencies is estimated to be in excess of 12 million. Among the state agencies, 18 of 21 disclosed that their volume of records containing personal information is in excess of 100,000. Of these, nine (9) state agencies reported volumes greater than 1 million and another five (5) agencies had volumes between 500,001 – 1,000,000

The nine (9) state agencies reporting record volumes greater than 1 million are Department of the Attorney General, Department of Commerce and Consumer Affairs, Department of Health, Department of Human Services, Department of Labor and Industrial Relations, Department of Land and Natural Resources, Department of Public Safety, Department of Taxation, and the Judiciary.

Lesser but still significant volumes of records were reported by the county agencies. In all, Honolulu agencies estimated the total volume of records maintained to be in excess of 5 million. 9 of 23 Honolulu agencies disclosed that their volume of records was in excess of 100,000. Of these, three (3) Honolulu agencies reported volumes greater than 1 million and another three (3) agencies had record volumes between 500,001 – 1,000,000.

The three (3) Honolulu agencies reporting record volumes greater than 1 million are Department of Information Technology, Department of Emergency Services, and the Honolulu Police Department. The three (3) Honolulu agencies with volumes between 500,001 – 1,000,000 are Office of the City Clerk, Customer Services Department, and Department of Parks and Recreation.

Four (4) Hawai'i county agencies reported record volumes in excess of 100,000 and one of them, Hawai'i Police Department had volumes greater than 1 million.

Two (2) Kauai agencies reported record volumes between 100,001 – 500,000 including Kauai Police Department and Kauai Department of Public Works.

And in Maui, three (3) agencies reported record volumes in excess of 500,000 with two (2) of them reporting volumes greater than 1 million. The latter include Maui Department of Finance and the Maui Department of Police.

Records Volume Growth

With respect to record volume growth, a distribution table representing state agency record volumes by estimated annual volume growths is displayed in *Table 3, Estimated State Agency Record Volumes by Annual Volume Growth*.

Volume Range	0%	1% - 5%	6% - 10%	11% - 25%	26% - 50%	Total
1 - 100	0	1	0	0	0	1
101 – 1,000	0	1	0	0	0	1
1,001 – 10, 000	0	0	0	0	0	0
10,001 – 100,000	0	0	0	1	0	1
100,001 – 500,000	0	2	0	0	1	3
500,001 – 1,000,000	0	2	2	1	0	5
1,000,001 or more	0	2	4	2	1	9
	0	8	6	4	2	20

Estimated State Agency Record Volumes By Annual Volume Growth

Table 3

All of the state agencies reported at least 1% - 5% volume growth in records containing personal information. Among the nine (9) state agencies reporting record volumes in excess of 1 million, four (4) including Department of the Attorney General, Department of Commerce and Consumer Affairs, Department of Land and Natural Resources, and Department of Taxation estimated annual volume growth to be 6% - 10%. Two (2) including the Department of Public Safety and the Judiciary reported annual volume growth to be 11% - 25%. And one (1), the Department of Health reported annual volume growth to be an estimated 26% - 50%.

A distribution table representing county agency record volumes by estimated annual volume growths is displayed in *Table 4, Estimated County Agency Record Volumes by Annual Volume Growth*.

Volume Range	0%	1% - 5%	6% - 10%	11% - 25%	26% - 50%	Total
1 - 100	3	3	0	1	0	7
101 – 1,000	0	8	3	0	0	11
1,001 – 10, 000	1	9	1	1	0	12
10,001 – 100,000	0	8	3	3	0	14
100,001 – 500,000	0	3	3	0	2	8
500,001 – 1,000,000	0	2	1	1	0	4
1,000,001 or more	0	3	2	1	0	6
	4	36	13	7	2	62

Estimated County Agency Record Volumes By Annual Volume Growth

Table 4

Four (4) county agencies with minimal record volumes reported 0% estimated annual growth. Of the six (6) county agencies reporting record volumes in excess of 1 million, three (3) estimated annual volume growth to be 1% - 6%. They include Honolulu Department of Information Technology, Honolulu Police Department, and Maui Police Department. Two (2) including Honolulu Department of Emergency Services and Maui Department of Finance reported volume growth estimates to be 6% - 10%. And one (1) county agency, Hawai'i Police Department estimated annual record volume growth to be 11% - 25%.

Section 4. Best Practices to Prevent Identity Theft

This section provides a summary of best practices to prevent identity theft that was identified through a review of other jurisdictions' activities, policies, and laws applicable to protecting personal information collected by government agencies. Specific emphasis is placed on best practices identified to protect social security numbers in situations including the sale, lease, trade, rent, or otherwise intentional release of an individual's social security number to a third party.

President's Task Force on Identity Theft Strategic Plan

In April, 2007 the President's Task Force on Identity Theft released *Combating Identity Theft: A Strategic Plan*²⁹. The document was developed by the Task Force in response to the charge to create a strategic plan aimed to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution.

While primarily addressing actions for the federal government, the strategic plan contains a number of recommendations that are relevant to protecting personal information managed by government agencies at the state and county levels. The recommendations pertinent to state/county governments are paraphrased and summarized below:

1. Decrease the unnecessary use of social security number. The Task Force recognized that there are many necessary or beneficial uses of the social security number (SSN). The SSN is often used to match individuals with their records and databases, including their credit files, to provide benefits and detect fraud. State and county governments rely extensively on SSNs when administering programs that deliver services and benefits to the public. While SSNs sometimes are necessary for legal compliance, other uses are more a matter of convenience or habit. In these cases, a different unique identifier generated by the organization could be equally suitable, but without the risk inherent in the SSN's use.

The Task Force recommended the following actions to limit the unnecessary use of SSNs in the public sector.

- a. Implement a complete review of use of SSNs.
 - b. Issue guidance on appropriate use of SSNs
 - c. Require agencies to review use of SSNs
 - d. Establish a clearinghouse for agency practices that minimize use of SSNs
 - e. Work with state and local governments to review use of SSNs.
2. Implement appropriate data security. The Task Force identified the critical role that the federal government's information privacy program and the information and information technology security program play in protecting personal information and preventing identity theft. While acknowledging that federal agency performance on information security has been uneven, the Task Force asserted that it is essential that agencies implement critical program components/initiatives to assure the security of personal information.

²⁹ President's Task Force on Identity Theft, *Combating Identity Theft: A Strategic Plan*, April 2007

Specifically referenced program components/initiatives include:

- a. Establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources.
- b. Provide for the development and maintenance of minimum controls required to protect information and information systems.
- c. Assign specific policy and oversight responsibilities.
- d. Require the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.
- e. Conduct an annual review of the agency information security program.
- f. Require agencies to prepare extensive data collection analyses and report periodically to the responsible executive and legislative branch oversight units.
- g. Implement employee training on security awareness topics.
- h. Develop comprehensive formal guidance to agencies on how to respond to data breaches.
 - i. Develop concrete guidance and best practices that ensure effective, risk-based responses to data breaches.
 - ii. Comply with data security guidance
 - iii. Protect portable storage and communications devices

With the selected recommendations from the President's Identity Theft Task Force strategic plan as a best practices reference point, information on laws and initiatives implemented by the states to protect personal information is presented in the sections that follow.

State Laws and Initiatives

A compilation of state initiatives and statutes identified is provided in *Appendix 4, Best Practices in Other State Jurisdictions*.

Assign Policy and Oversight Responsibilities

Eight (8) states have assigned identity theft related responsibilities to specifically designated government organizations. These are identified in *Table 5, Identity Theft – Assigned State Agencies*.

California's Office of Privacy Protection was created as a unit of the Department of Consumer Affairs in 2001. An excerpt from the statutory provisions authorizing the formation of this agency is provided in *Exhibit 2, State of California Business and Professions Code, Section 350-352*.

Among the main purposes of the California Office of Privacy Protection are:

1. Assist individuals with identity theft and other privacy-related concerns.
2. Provide consumer education and information on privacy issues.
3. Coordinate with local, state and federal law enforcement on identity theft investigations.
4. Recommend policies and practices that protect individual privacy rights.

	State	Agency
1	California	Office of Privacy Protection
2	Colorado	Identity Theft and Financial Fraud Unit
3	Connecticut	The Governor's Identity Theft Information Team
4	Kentucky	Financial Integrity Enforcement Division
5	Maryland	Office of the Attorney General, Electronic Transaction Education, Advocacy, and Mediation Unit
6	Michigan	Michigan State Police, Identity Theft Unit
7	Minnesota	Financial Crimes Oversight Council and Task Force
8	Wisconsin	Office of Privacy Protection

Identity Theft – Assigned State Agencies
Table 5

This agency is notable for the breadth and quality of initiatives that it has sponsored since its inception. For the period 2005 - 2006, the California Office of Privacy Protection reported that it prepared six (6) Consumer Information Sheets; implemented 50 workshops and seminars for consumer/community groups and 41 for business/government/professional groups; prepared or updated three (3) best practice documents (*Recommended Practices on Notice of Security Breach*, *A California Business Privacy Handbook*, *State Government Privacy Practices Handbook*); provided consumer assistance by responding to 5,015 calls/emails/letters; and providing security breach assistance by responding to 1,117 calls and emails.

Colorado³⁰ has created the Identity Theft and Financial Fraud unit within its Department of Public Safety. The assigned purpose for this office is to supplement the existing law enforcement and prosecution system and provide flexibility to respond to the shifting aspects of identity theft and financial fraud crimes and priorities among such crimes. The unit also provides to the public information about financial fraud and the unit's activities and results.

Connecticut created the Identity Theft Information Team in 2006 in the wake of the security breach incident at the United States Veterans Administration. The purpose of this special purpose unit is to host identity theft prevention seminars to inform veterans and members of the military on how to protect themselves from being victims of identity theft.

Kentucky³¹ has the Financial Integrity Enforcement Division among whose duties are to investigate the use of personal information and financial information by persons for the purpose of theft, or fraud, or both theft and fraud, and other illegal or fraudulent activity which may involve electronic commerce.

Maryland has the Electronic Transaction Education, Advocacy, and Mediation Unit in the Office of the Attorney General. The purpose of the unit is to protect the privacy of individuals' personal information and to protect the public from unlawful conduct or practices in electronic transactions.

Among the stated duties of the Maryland unit are:

³⁰ 24-33.5-1702. Legislative declaration

³¹ <http://www.lrc.ky.gov/krs/015-00/113.pdf>

1. Receive complaints concerning personal information that may potentially involve unlawful acts or violate a stated privacy policy.
2. Provide information and advice to the public on effective ways of handling complaints that involve violations of privacy related laws, including identity theft and identity fraud or unlawful conduct or practices in electronic transactions.
3. Refer privacy and electronic transactions related complaints where appropriate to local, State, or federal agencies.
4. Develop information and educational programs and materials to foster public understanding and recognition of the issues related to privacy in electronic commerce and unlawful conduct or practices in electronic transactions.
5. Identify consumer problems in, and facilitate the development and use of best practices by persons engaged in electronic commerce for the protection of the privacy of personal information in electronic transactions.
6. Promote voluntary and mutually agreed upon nonbinding arbitration and mediation of privacy related or electronic transaction disputes where appropriate.
7. Investigate and assist in the prosecution of identity theft and other privacy related crimes.
8. Assist and coordinate in the training of local, State, and federal law enforcement agencies regarding identity theft, other privacy related crimes, and unlawful conduct or practices in electronic transactions as appropriate.

Michigan³² has created the Identity Theft Unit within the Michigan State Police. The purpose of the unit is to assist federal and local law enforcement agencies with investigating criminal identity theft and to provide victims with available resources to prevent further victimization.

Minnesota³³ has the Financial Crimes Oversight Council and Task Force. This group is composed of senior legal and law enforcement officials and representatives from the private sector. Among its duties are to develop an overall strategy to ameliorate the harm caused to the public by identity theft and financial crime in Minnesota, assist law enforcement agencies and victims in developing a process to collect and share information to improve the investigation and prosecution of identity theft and financial crime.

In April 2006, Wisconsin created the Office of Privacy Protection. While similar in purpose as the California entity, the Wisconsin office also has substantial operational assignments including:

1. To protect the privacy of individuals' personal information by identifying consumer problems and facilitating the development of fair information practices
2. To provide information and assistance, where appropriate, to consumers in reclaiming their identity and clearing their name in the event of identity theft or identity fraud
3. To maintain a database of consumer complaints on issues of identity theft, identity fraud, and other privacy related issues
4. To investigate and assist in the prosecution of identity theft and other privacy related laws, and, as necessary and appropriate, coordinate with local, state, and federal law enforcement agencies in the investigation of similar violations
5. To make recommendations to organizations for privacy policies and practices that promote and protect the interest of Wisconsin consumers and businesses

³² http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html

³³

http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006§ion=299A.681&keyword_type=exact&keyword=identity+theft

6. To promote voluntary mediation of privacy related disputes where appropriate
7. To receive complaints from individuals concerning any person's obtaining, compiling, maintaining, using, disclosing or disposing of personal information that may be potentially unlawful, and provide advice, information, and referral where available

Decrease the Unnecessary Use of SSN

Many of the states have been proactive in initiating laws and practices to decrease the use of SSN by public sector agencies.

California was an early participant in this effort with its adoption of Civil Code Sections 1798.85-1798.86 in 2002. Among other things, this statute includes prohibitions of the following practices:

1. Posting or publicly displaying of SSNs
2. Printing SSNs on identification cards or badges
3. Requiring people to transmit an SSN over the Internet unless the connection is secure or the SSN is encrypted.
4. Requiring people to log onto a website using an SSN without a password
5. Printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.

To support compliance with the California laws on SSN confidentiality, the California Office of Privacy Protection published *Recommended Practices on Protecting the Confidentiality of Social Security Numbers*³⁴ in 2007. Among the recommendations to both private and public sector organizations are the following:

1. Reduce the collection of SSN
 - a. Collect SSNs preferably only where required to do so by federal or state law.
 - b. When collecting SSNs as allowed, but not required, by law, do so only as reasonably necessary for proper administration of lawful business activities.
 - c. If a unique personal identifier is needed, develop your own as a substitute for the SSN.
2. Inform individuals when you request their SSNs
 - a. Whenever you collect SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number.
 - b. If required by law, notify individuals annually of their right to request that you do not post or publicly display their SSN or do any of the other things prohibited in Civil Code Section 1798.85(a).
3. Eliminate the public display of SSNs
 - a. Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.

³⁴ California Department of Consumer Affairs, Office of Privacy Protection, *Recommended Practices on Protecting the Confidentiality of Social Security Numbers*, April 2007, (<http://www.privacyprotection.ca.gov/recommendations/ssnrecommendations.pdf>)

- b. Do not send documents with SSNs on them through the mail, except on applications or forms or when required by law.
 - c. When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
 - d. Do not send SSNs by email unless the connection is secure or the SSN is encrypted.
 - e. Do not require an individual to send his or her SSN over the Internet or by email, unless the connection is secure or the SSN is encrypted.
 - f. Do not require individuals to use SSNs as passwords or codes for access to Internet websites or other services.
4. Control access to SSNs
- a. Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
 - b. Use logs or electronic audit trails to monitor employees' access to records with SSNs
 - c. Protect records containing SSNs, including backups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
 - d. Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
 - e. Avoid sharing SSNs with other companies or organizations except where required by law.
 - f. If you do share SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.
 - g. Prohibit such third parties from redisclosing SSNs, except as required by law.
 - h. Require such third parties to use effective security controls on record systems containing SSNs.
 - i. Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.
 - j. If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.
5. Protect SSNs with security safeguards
- a. Develop a written security plan for record systems that contain SSNs
 - b. Develop written policies for protecting the confidentiality of SSNs, including but not limited to the following:
 - i. Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
 - ii. Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.

- iii. Require employees to ask individuals for identifiers other than the SSN when looking up records for the individual.
 - iv. Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.
 - v. When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.
- c. Make your organization accountable for protecting SSNs
- i. Provide training and written material for employees on their responsibilities in handling SSNs
 - ii. Conduct training at least annually.
 - iii. Train all new employees, temporary employees and contract employees.
 - iv. Impose discipline on employees for non-compliance with organizational policies and practices for protecting SSNs.
 - v. Conduct risk assessments and regular audits of record systems containing SSNs
 - vi. Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.

Nevada has adopted statutory provisions³⁵ affecting the use of SSNs by government agencies in documents that state:

1. Persons shall not be required to include the social security number of a person on any document that is recorded, filed or otherwise submitted to a government agency on or after January 1 2007.
2. If SSNs are required, then the government agency shall maintain the SSN in a confidential manner and may only disclose the SSN under specific, limited circumstances.
3. Agencies shall provide appropriate notice to individuals regarding the restricted use of SSN.
4. Agencies may require individuals to provide affirmations that documents submitted to government agencies do not include SSN and may refuse documents that do not have the affirmation or that contain SSN.

In North Carolina, agencies are directed to collect SSN and other personal identifying information only for legitimate purposes or when required by law.³⁶ Further, state agencies may not:

1. Collect a social security number from an individual unless authorized by law to do so or unless the collection of the social security number is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

³⁵ Nevada Revised Statutes Section 239B.030 Confidentiality of social security numbers. [Effective January 1, 2007.]

³⁶ North Carolina General Statutes § 132-1.10. Social security numbers and other personal identifying information.

2. Fail, when collecting a social security number from an individual, to segregate that number on a separate page from the rest of the record in order that the social security number can be more easily redacted pursuant to a valid public records request.
3. Fail, when collecting a social security number to provide a statement of the purpose or purposes for which the social security number is being collected and used.
4. Use the social security number for any purpose other than the purpose stated.

Ohio has a general prohibition³⁷ to including SSN in documents that are to be recorded. In Ohio, preparers are directed that they shall not include any individual's social security number in any document that is to be filed for recording in the office of the county recorder and the county recorder shall not accept such a document for recording that includes any individual's social security number.

Other examples of state efforts to reduce the use of SSN include New Jersey³⁸ which prohibits state agencies from publicly displaying social security number or any four or more consecutive digits from the social security number and Pennsylvania which has terminated the practice of printing social security numbers on unemployment compensation checks and.

Reduce Information Technology Security Risks to an Acceptable Level

In addition to their efforts to reduce the use of SSNs, some states have implemented statutes and initiatives to more generally limit the scope of information collected and maintained by agencies.

In California, agencies are directed to

1. Limit the personal information that is maintained in agency records to that which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.³⁹
2. Collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source.⁴⁰

Indiana has issued similar guidance to its agencies⁴¹. As applied to personal information systems maintained by any state agency, Indiana agencies are to:

1. Collect, maintain, and use only that personal information as is relevant and necessary to accomplish a statutory purpose of the agency.
2. Collect information to the greatest extent practicable from the data subject directly when the information may result in adverse determinations about an individual's rights, benefits and privileges under federal or state programs;
3. Collect no personal information concerning in any way the political or religious beliefs, affiliations and activities of an individual unless expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to IC 4-22-2.

³⁷ Ohio Revised Code Section 317.082 Social security number not to be included in document filed for recording

³⁸ New Jersey Statutes C.56:8-164 Prohibited actions relative to display of social security numbers

³⁹ California Civil Code Section 1798.14

⁴⁰ California Civil Code Section 1798.15

⁴¹ Indiana Code 4-1-6-2

In 2006, Missouri enacted a statute⁴² that restricts the inclusion of *sensitive* personal information in recorded documents. A significant provision in the statute is the stipulation that the redaction or the removal of such sensitive personal information shall not affect the legal status of the transaction represented by the document.

A copy of the Missouri statute is presented in *Exhibit 3, Chapter 59 County Recorders of Deeds*.

Virginia has more prescriptive statutory guidance⁴³ on the administration of systems that include personal information. Among other requirements, Virginia agencies are directed to:

1. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;
2. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to ensure fairness in determinations relating to a data subject;
3. Make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto, and (ii) receiving reasonable assurances that those requirements and limitations will be observed.

In Wisconsin⁴⁴, agencies that maintain an Internet site may not use that site to obtain personally identifiable information from any person who visits that site without the consent of that person.

Establish a Comprehensive Framework for Ensuring the Effectiveness of Information Security Controls Over Information Resources

California is a best practice leader among the states with regard developing a comprehensive system to protect personal information. The California Information Practices Act of 1977⁴⁵, which provides the foundation for government agency information practices in California, demonstrates a clear commitment to deploy systems and controls to protect the privacy and confidentiality of individuals' personal information.

A complete copy of the California Information Practices Act of 1977 is presented in *Exhibit 4, California Information Practices Act of 1977*.

Significant features of the California information practices standard include:

1. Applies to all records that may be any file or grouping of information about an individual that is maintained by an agency by reference to an identifying particular such as the individual's name, photograph, finger or voice print, or a number or symbol assigned to the individual.
2. Stipulates that agencies that collect personal information shall maintain the source or sources of the information.
3. In general, agencies, on forms used to collect personal information from individuals, shall provide a notice that contains agency contact information; the location of records and the categories of persons who may use those records; the authority which authorizes the maintenance of the information; whether submission of such information is mandatory or voluntary; the consequences, if any, of not providing all or any part of the requested information; the principal purposes for which the information is to be used, disclosures

⁴² Missouri Revised Statutes, Chapter 59, County Recorders of Deeds, Section 59.331

⁴³ Virginia Code § 2.2-3803. Administration of systems including personal information; Internet privacy policy; exceptions.

⁴⁴ Wisconsin Statutes 19.68 Collection of personally identifiable information from Internet users

⁴⁵ California Civil Code Section 1798 – 1798.78

which may be made of the information, and the individual's right of access to records containing personal information which are maintained by the agency.

4. Agencies must ensure that when records are transferred to third parties in support of agency operations, that contractual agreements are implemented that require the third parties to deploy similar safeguards as required of the agency.
5. Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.
6. Each agency shall designate an agency employee to be responsible for ensuring that the agency complies with all of the provisions of this chapter.
7. Agencies are constrained from disclosing personal information that would link the information to the individual to whom it pertains except under specified, restricted circumstances.
8. Agencies shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made, with noted exceptions.
9. The intentional violation of any provision of this chapter or of any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.
10. An individual's name and address may not be distributed for commercial purposes, sold, or rented by an agency unless such action is specifically authorized by law.

With regard personal information use policies, other states, in addition to California, that require notices to individuals include Delaware⁴⁶, Indiana⁴⁷, Iowa⁴⁸, Maine⁴⁹, Maryland⁵⁰, and Virginia⁵¹.

Virginia includes an additional requirement⁵² to maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained.

Many of the states provide agencies with an exemption from mandated personal information protection provisions when the agency is subject to other state or federal laws that are as stringent or more stringent. As an example Arkansas⁵³ has a preemption provision that exempts agencies regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by its disclosure of security breaches requirements.

⁴⁶ Delaware Code 9018C. Development and implementation of agency privacy policies

⁴⁷ Indiana Code 4-1-6-2 Personal information system

⁴⁸ Iowa Code 61-2.8(17A.22) Notice to suppliers of information

⁴⁹ Maine Revised Statutes Chapter 14-A: Notice of Information Practices

⁵⁰ Maryland Code 10-624 Personal Records

⁵¹ Virginia Code 2.2-3803

⁵² Virginia Code 2.2-3803

⁵³ Arkansas Code 4-110-105

Require Agencies to Prepare Extensive Data Collection Analyses and Report Periodically to the Responsible Executive and Legislative Branch Oversight Units

A significant feature in the Indiana Fair Information Practices Act ⁵⁴ is a requirement that Indiana agencies must file an annual report with the general assembly on the existence and character of each system added or eliminated since the last report with the governor on or before December 31. Among the required elements of the annual report are a description of personal information systems, justification for the system, the categories of personal information held, and the identity of agency personnel who have access

Like Indiana, New Hampshire requires that its agencies file an annual report⁵⁵ with the Secretary of State on personal information systems. Elements that must be included in this annual report include:

1. The name of the system.
2. The purpose of the system.
3. The number of persons on whom personal information is maintained in the system.
4. Categories of personal information maintained in the system.
5. Categories of the sources of the personal information in the system.
6. Descriptions of the uses made of the personal information.
7. Categories of users of the personal information.
8. Practices regarding the place and method of personal information storage in the system including but not limited to whether or not the personal information is machine-accessible.
9. Length of time of retention of personal information in the system.
10. Method of disposal of personal information in the system.
11. Names and positions of the personnel responsible for maintaining the system.
12. Persons or agencies having a right of access to the personal information in the system.

Implement Agency Training on Security Awareness Topics and on How to Respond to Data Breaches

The states have taken varied approaches to presenting information to agencies on protecting personal information and on how to respond to data breaches.

Websites are a common delivery vehicle used by the states. Among the states that provide educational information on identity theft on their websites are Arizona, California, Colorado, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Washington, and Wisconsin. Links to those websites are provided in *Appendix 2, Best Practices in Other State Jurisdictions*.

⁵⁴ Indiana Code 4-1-6 Fair Information Practices, Privacy of Personal Information

⁵⁵ New Hampshire Revised Statutes Chapter 7-A, Information Practices Act

California, Ohio, Pennsylvania have particularly well developed websites offering assistance to consumers. Pennsylvania's website called the Identity Theft Action Plan offers individuals detailed guidance on preventing and responding to identity theft events.

Among the states, only California has developed content specifically directed to state employees. On its website, the California Office of Privacy Protection publishes information for state government employees on privacy practices and policies for protecting personal information on its website. A snapshot of the website is provided below.



Among the topics presented on the Office of Privacy Protection website for state employees are:

1. Protecting Privacy in State Government. Basic Training for State Employees
 - a. PowerPoint Presentation
 - b. Self-Training Manual
 - c. Guidelines for Self-Training Manual
2. Data Classification and Privacy Inventory.
 - a. Training PowerPoint Presentation
 - b. Privacy Inventory Worksheet
 - c. Privacy Inventory Instructions
3. Information on Security Breach Notification
 - a. Security Incident Notification Steps –
 - b. Breach Response Call Center FAQs
 - c. Security Breach Notice Recommended Practices (including Sample Notices)
 - d. Security Breach First Steps

Besides website based education initiatives, states have provided varied levels of support for workshops and materials to educate agencies, community groups and businesses on identity theft related issues.

In 2006, the California Office of Privacy Protection developed a number of (bilingual) consumer education materials, conducted over 100 workshops for consumer/community groups and business/government/professional groups, and held an annual identity theft summit attended by nearly 1,000.

Also in 2006, the Identity Theft Teams of the Michigan State Police (MSP) in conjunction with the Michigan Association of Chiefs of Police (MACP) and the Michigan Sheriff's Association (MSA) delivered a four hour training session at several locations in the state that offered information on investigating identity theft, credit fraud and counterfeiting complaints.

Mitigate the Impact of Security Breaches

Twenty five (25) of the states have enacted legislation that requires a notification in cases when a security breach has occurred. In some states, the notification threshold is triggered when a breach has been detected. As an example, in Oklahoma⁵⁶:

Any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Oklahoma whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection C of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

⁵⁶ Oklahoma Statutes §74-3113.1, Disclosure of breach of security of computerized personal information

In other states, the notification requirement is only required if there is a reasonable suspicion that there may be harm to individuals. This is the case in Hawaii.

Arkansas⁵⁷, Delaware⁵⁸, Iowa⁵⁹, Maryland⁶⁰, Montana⁶¹, Nevada⁶², Oklahoma⁶³, and Virginia⁶⁴ have created the identity theft passport for victims of identity theft. With some state variations, after an identity theft victim has filed a police report with the local law enforcement agency, the victim may apply for an identity theft passport by sending a copy of the police report and an application form.

Upon receipt of the identity theft passport, the identity theft victim may present it to a law enforcement agency to help prevent the victim's arrest/detention of an offense committed by a person other than the victim, who is using the victim's identity; or to a creditor of the victim to aid in the creditor's investigation and establishment of whether a fraudulent charge was made against an account in the victim's name; or to any other entity to aid in the entity's investigation of whether the victim's identity was fraudulently obtained or used without the victim's consent.

In a similar initiative, California offers the California Identity Theft Registry⁶⁵ to help victims of identity theft who are wrongly linked to crimes. The registry provides a centralized place that can be checked by police and other authorized persons to confirm that an individual is not wanted by law enforcement and that a mistaken criminal history was created in that person's name.

An example of how an individual might become a victim of "criminal" identity theft:

1. The thief is cited or arrested for a crime and uses the individual's name for police records.
2. The thief is charged and prosecuted in that individual's name so that name now appears in court records.
3. The thief is convicted in that name of a crime.
4. That name is somehow mistakenly associated with a record of a criminal conviction of some other individual.

If victimized, the individual may be able to correct the problem by presenting information on the identity theft to the California law enforcement agency that requested issuance of the arrest warrant. Otherwise, the individual would need to go to court for a finding of factual innocence. Then the individual could apply to have this court finding entered into the California ID Theft Registry.

Georgia⁶⁶ offers a similar repository which is maintained by the Governor's Office of Consumer Affairs. This repository contains information compiled during the course of investigations conducted by the Office of Consumer Affairs. The information is not for public disclosure but is available to authorized law enforcement and prosecutorial agencies.

Texas⁶⁷ offers victims of identity theft an option to file an application with a district court for the issuance of a court order declaring that the person is a victim of identity theft. Upon due hearing and consideration, the court may issue an order declaring the individual a victim of identity theft along with pertinent information regarding the identity theft circumstance. The order may be

⁵⁷ Arkansas Code 5-37-228. Identity theft passport

⁵⁸ Delaware Code 854A. Identity theft passport

⁵⁹ Iowa Code 715A.9A Identity Theft Passport

⁶⁰ Maryland Code 8-305 Identity theft passport

⁶¹ Montana Code 46-24-220 Identity theft passport

⁶² Nevada Revised Statutes 205.4651 Identity theft passport

⁶³ Oklahoma Statutes 22-19b. Oklahoma identity theft passport program

⁶⁴ Virginia Code 18.2-186.5

⁶⁵ California Civil Code Section 530.7

⁶⁶ Georgia Code 167-9-123. Investigations

⁶⁷ Texas Code § 48.202

opened and made available to officials in a civil proceeding or to the victim for presentation to a government entity or private business to prove that a financial transaction or account of the victim was affected by a violation of identity theft statutes.

The Utah⁶⁸ attorney general manages an identity theft report information system website where victims of an identity-related crime may report the crime and have the victim's report routed to the appropriate law enforcement agency for the jurisdiction in which the crime occurred.

In Illinois, the Office of Illinois Attorney General created the Illinois Identity Theft Hotline⁶⁹. The hotline provides citizens who have been victimized by identity theft with one-on-one assistance to take the steps necessary to report the crime to local law enforcement and financial institutions, repair their credit, and prevent future problems.

In an initiative designed to provide financial relief to identity theft victims from debt collectors, California enacted statutes⁷⁰ that protect identity theft victims who are being pursued for collection of debts which have been created by identity thieves. A copy of the statute is presented in *Exhibit 5, California Civil Code § 1788.18*.

The law gives identity theft victims the right to bring an action against a claimant who is seeking payment on a debt not owed by the identity theft victim. The identity theft victim may seek an injunction against the claimant, plus actual damages, costs, a civil penalty, and other relief. Additionally, the law provides a process whereby a debtor may submit to a debt collector either a copy of a police report alleging that the debtor is the victim of an identity theft crime, or a written statement by the debtor that claims that the debtor is a victim of identity theft with respect to the specific debt being collected. Upon receipt of the police report and/or debtor statement, the debt collector then may make an assessment and either resume/cease collection activities.

And in Texas, there is a statute⁷¹ that requires that the Department of Mental Health and Mental Retardation to implement a system that assures that investigations that affect mental health/aged clients and that involve complex issues including identity theft are (1) assigned to personnel who have experience and training in those issues and (2) monitored by a special task unit for complex cases.

⁶⁸ Utah Code 67-5-22. Identity theft reporting information system

⁶⁹ Attorney General ID Theft Resource Guide,
http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf

⁷⁰ California Civil Code Section 1798-92 to 1798-97

⁷¹ Texas Code § 48.1521. Investigation of Complex Cases

Section 5. Risk Assessment and Findings

To assess the risk and impact of unauthorized disclosures based on the volume of personal information collected and maintained by Hawai'i state and county agencies, questions⁷² were included in the January 2007 personal information survey to ascertain the following:

1. Personal information collected by agencies.
2. The volume and growth of records containing personal information used by Hawai'i agencies.
3. Patterns of personal information use and disclosure by agencies.
4. Physical means deployed by agencies in the use and disclosure of personal information.
5. The types and extent of technical safeguards used by agencies when transmitting personal information.
6. The extent that agreements contain provisions to assure appropriate safeguard are deployed to protect personal information when third parties are used to perform activities on behalf of agencies.
7. The extent that agencies deploy specific written policies and procedures to safeguard personal information used/disclosed in agency business processes.

Personal Information Collected by Agencies

A critical factor for reducing the risk of unauthorized disclosures is to limit the scope of personal information collected and maintained by agencies.

As a means to reduce their risks to security breaches, other state jurisdictions have implemented statutory initiatives that limit the personal information that is maintained in agencies to that which is relevant and necessary to accomplish a purpose of the agency, authorized by statute or mandated by the federal government. Some of the states have also been proactive in initiating laws and practices specifically directed toward decreasing the use of SSN by agencies. In some states, agencies are required to make annual reports to their state legislatures as a means to support legislative oversight/control on agency collection/use of personal information. And, some states have enacted statutory provisions that restrict the inclusion of SSN in documents submitted to agencies for public recordation.

Hawai'i does not have comparable statutory provisions that would have the effect of limiting the personal information that is collected and maintained by agencies. In the absence of such provisions, Hawai'i is reliant on state and county agency management when it comes to controlling the scope of personal information collected and maintained.

In the January 2007 personal information questionnaire, agencies were queried on whether their units *limit the use or disclosure of personal information to only that which is necessary to carry out the intended purpose*. All responding agencies replied in the affirmative.

⁷² Research note: In some instances, questionnaires were received for subunits within departments. The questionnaires from these subunits were aggregated into a single department response. For questionnaire items requesting a YES/NO response, a YES or NO was recorded if that was the consensus response from all subunits within the department. If there was a mixed YES and NO response from the subunits, then that was taken as an indication that no department-wide policy/practice had been deployed and a NO response was recorded for the item.

Volume and Growth of Records

From a security perspective, the volume of records containing personal information that may be used/disclosed by agencies does not, in and of itself, represent a risk factor. The relative risk of unauthorized use/disclosure of personal information is more a function of defined security threats and the safeguards that are deployed to counter those threats.

That being said, the volume and/or growth of records containing personal information do affect the impact of security breaches on agencies in significant ways. The total number of individuals about whom personal information is used/disclosed in agency records represents the threshold number of individuals whose information could be exposed to an identity theft event and who would need to be notified in the case of a security breach. Generally, higher volumes of documents/records will correlate with higher numbers of individuals that may be impacted by a security breach.

Agencies may have a higher risk exposure if they use/maintain large volumes of documents/records containing personal information dispersed across multiple agency sites/systems and have not deployed appropriate administrative, technical, and physical safeguards at each site.

Agencies with large volumes of documents/records containing personal information may have a higher risk profile if the personal information is used/disclosed over Internet websites and adequate administrative and technical safeguards have not been deployed. They may also have a higher risk exposure if the personal information is transmitted electronically without appropriate technical safeguards to protect the information from unauthorized access during transmission.

If agencies routinely store personal information on portable computer devices (e.g. laptops, smart phones) and/or removable electronic storage media (floppy disks, CD-ROM, portable hard drives, tapes, USD drives) and have not deployed appropriate administrative, technical, and physical safeguards, they may have a higher risk profile.

Agencies using third party entities to perform activities on their behalf (financial reviews, audits, actuarial studies, IT outsourcing), where access to large volumes of documents/records is required, may have a high risk exposure if agreements are not put in place to assure appropriate safeguards are used by the third party entity.

And to the extent that agencies fail to deploy appropriate safeguards due to the relatively greater costs involved in protecting large volumes of documents/records, then they may be exposed to higher levels of security risks.

As presented in Section 3 *Personal Information – Agency Usage and Practices*, Hawai'i state and county agencies, individually and in aggregate, collect and maintain a substantial volume of documents/records containing personal information. Among the 105 Hawai'i state and county agencies surveyed in January 2007, 75 of 89 (84%) responding agencies reported that they handled, processed, or stored documents/records containing personal information within their agency.

Of these, fifteen (15) reported volumes in excess of 1 million and nine (9) had volumes between 500,001 – 1,000,000. Significantly, among the agencies with document/record volumes greater than 1 million, ten (10) estimated that annual volume growth rates would exceed 6% - 10%.

Absent initiatives to stem the projected annual growth and notwithstanding records archiving/disposal, the volume of documents/records containing personal information collected/maintained by Hawai'i agencies can reasonably be expected to grow to highly significant levels in the coming years. To illustrate the point, the estimated volumes for the fifteen (15) agencies reporting 2007 document/record volumes in excess of 1 million, were computed using the reported low end estimated annual volume growth rates for 5, 10, and 20 years in the future.

The results are presented in *Table 6, Volume Growth Estimates - Agencies (> 1,000,000 Document/Records, 2007)*.

From a baseline of approximately 15 million records in 2007, the total volume of records for the fifteen (15) agencies is projected to grow to over 21 million in five (5) years time, over 35 million in ten (10) years and to over 153 million records in twenty (20) years.

Patterns of Use and Disclosures

Notwithstanding the safeguards that may be deployed, agencies have a relatively greater risk exposure to external source security threats when documents/records are transmitted and/or transported from their custodial agencies. During transport/transmittal, hard copy documents/records and documents electronically stored on portable computers/storage devices may be subject to theft, loss, data corruption or tampering. And electronic documents/records transmitted over networks may be accessed by or exposed to external agents.

In the event that security safeguards are not deployed uniformly throughout a department, there may be risks to unauthorized access when personal information is transmitted/transported to/from other units within a department. And there may be relatively greater security risks if the personal information is transmitted to an outside entity that lacks a comparable level of security safeguards.

In the January 2007 personal information questionnaire, state and county agencies were queried on their personal information use/disclosure⁷³. Agency responses are summarized below.

Does your unit receive personal information from other units in the department?

57 of 75 (76%) agencies replied in the affirmative.

1. Department of Education. Employment background check documents including fingerprint information form, FBI fingerprint card, employment eligibility verification. Employment forms.
2. Department of Hawaiian Home Lands. Application files and lessee files. Loan and lessee payments.
3. Department of Health. Personnel forms including recruitment, payroll, and automobile mileage. Vendor payments. Client and Medicaid eligibility information.
4. Department of Human Services. Employment background check documents. Workers compensation claims. Client applications for financial, food stamps and medical assistance.
5. Department of Labor and Industrial Relations. Unemployment insurance claims. Employee records. Workers compensation.
6. Department of Land and Natural Resources. Personnel forms. Licensing and permit information.
7. Judiciary. Public Guardian and Probate Court information. Juvenile client services information.

⁷³ Research note: For the analysis, responses were compiled for all state and county agencies. However, in this report section, only the responses from state agencies are summarized.

Agency	Annual Growth	2012	2017	2027
Department of the Attorney General	6% - 10%	1,338,226	1,790,848	3,207,135
Department of Commerce and Consumer Affairs	6% - 10%	1,338,226	1,790,848	3,207,135
Department of Commerce and Consumer Affairs	6% - 10%	1,338,226	1,790,848	3,207,135
Department of Health	26% - 50%	3,175,797	10,085,686	101,721,066
Department of Human Services	1% - 5%	1,051,010	1,104,622	1,220,190
Judiciary	11% - 25%	1,685,058	2,839,421	8,062,312
Department of Land and Natural Resources	6% - 10%	1,338,226	1,790,848	3,207,135
Department of Public Safety	11% - 25%	1,685,058	2,839,421	8,062,312
Department of Taxation	6% - 10%	1,338,226	1,790,848	3,207,135
Honolulu Department of Information Technology	1% - 5%	1,051,010	1,104,622	1,220,190
Honolulu Department of Emergency Services	6% - 10%	1,338,226	1,790,848	3,207,135
Honolulu Police Department	1% - 5%	1,051,010	1,104,622	1,220,190
Hawai'i County Police Department	11% - 25%	1,685,058	2,839,421	8,062,312
Maui County Department of Finance	6% - 10%	1,338,226	1,790,848	3,207,135
Maui County Department of Police	1% - 5%	1,051,010	1,104,622	1,220,190
TOTAL		21,802,591	35,558,372	153,238,709

Volume Growth Estimates - Agencies (> 1,000,000 Document/Records, 2007)

Table 6

Workforce application and employment information is a common document/record cited by state and county agencies as transmitted by agency units to department human resources and/or administrative services offices. While only 76% of agencies replied in the affirmative to this question, it is probable that all state and county agencies transmit personnel related information.

Other document/record types cited are client applications for loans, leases, and licenses and client case records. Typically, these client record types are circulated between agency units for services review/approval and case management purposes.

Does your unit transmit personal information to other units in the department?

58 of 75 (77%) agencies replied in the affirmative.

1. Department of Accounting and General Services. Personnel information. Data entry information. Payroll information. Procurement documents.
2. Department of Agriculture. Payroll information.
3. Department of Attorney General. Debtor information. Personnel information. Case information.
4. Department of Budget and Finance. Employee benefits enrollment forms.
5. Department of Business Economic Development & Tourism. Personnel information. Contracts information
6. Department of Commerce and Consumer Affairs. Business registration information. Personnel information. Producer license information. Consumer protection information.
7. Department of Defense. Personnel information.
8. Department of Education. Personnel information. Employee background check information.
9. Department of Hawaiian Home Lands. Loan and lessee information.
10. Department of Health. Personnel information. Patient information. Client and Medicaid eligibility information. Death information.
11. Department of Human Services. Employee background check information. Personnel information. Client and Medicaid information.
12. Department of Labor and Industrial Relations. Case hearings information. Unemployment, workers compensation and disability compensation case information.

As with the prior question, workforce and personnel related documents/records are reported to be commonly transmitted from agency units to department human resource and/or administrative services offices.

Does your unit receive personal information from outside your organization?

72 of 75 (96%) agencies replied in the affirmative.

1. Department of Accounting and General Services. Employee information (employees). Insurance claim information (health care providers). Procurement information (contractors and vendors).
2. Department of Agriculture. Employment verification (employers). Credit reports (TransUnion).
3. Department of Attorney General. Debt collections information (state agencies) including tax returns and child support case information.

4. Department of Budget and Finance. Personnel information (state agencies). Employee retirement (retirement applicants and retirees) and benefits information (employees, carriers).
5. Department of Business Economic Development & Tourism. Personnel information (state agencies). Financial (financial institutions) and credit reports (credit reporting agencies) information. Contracts (vendors and contractors) and labor services (temporary employment agencies) information. Property purchase applications (applicants) information.
6. Department of Commerce and Consumer Affairs. Business registration (licensing and law enforcement agencies) and licensing (regulatory agencies e.g. NASD-CRD/IARD, CSEA) information. Consumer complaints (complainants, law enforcement agencies) and administrative hearings information.
7. Department of Defense. Employment information (applicants/employees). Child support (CSEA) and protective services (child protective service agencies) information.
8. Department of Education. Personnel information (employers). Background check information (Hawai'i Criminal Justice Data Center, FBI). Payroll information (Employment Retirement System, DAGS).
9. Department of Health. Health care facility complaints (complainants, facilities) and investigation information. Medical insurance (payers) and patient information. Death certificate (mortuaries) information. WIC applicant (applicants) information. Personnel and employment background check (adult protective services agencies, child welfare services agencies) information.
10. Department of Human Resources Development. Payroll and personnel information (state agencies, HSTA).
11. Department of Human Services. Medicaid eligibility (applicants) information. Personnel (Attorney General, FBI, District Court, physicians, employers) information. Child support enforcement case (motor vehicle agency, financial institutions) information. Social services (Social Security Administration) case information.
12. Department of Labor and Industrial Relations. Refugee resettlement case (applicant) information. Employment services appeals and labor case (interested parties) information. Disability compensation (claimants), unemployment insurance (claimants), and job training (applicants, employers, labor unions) case information.
13. Judiciary. Case (parties with interest) information

A significant portion of personal information reported disclosed to agencies is from other state/federal agencies. Several state agencies including the Department of Accounting and General Services, Department of Attorney General, Department of Budget and Finance, and the Department of Human Resources Development provide support services to other state agencies and commonly receive document/records containing personal information related to their functional responsibilities from the other agencies.

Agencies receiving personal information on a recurring basis from non-government sources include Department of Agriculture (TransUnion credit reporting agency), Department of Budget and Finance (benefits carriers), Department of Commerce and Consumer Affairs (regulatory agencies, law enforcement agencies), Department of Education (FBI), Department of Health (payers), Department of Human Resources Development (HSTA), Department of Human Services (FBI, physicians, Social Security Administration), and Department of Labor and Industrial Relations (labor unions).

Does your unit transmit personal information outside your organization?

73 of 75 (97%) replied in the affirmative.

1. Department of Accounting and General Services. State employee tax withholding (Internal Revenue Service, Department of Taxation) information. Employee retirement information (Employees' Retirement System).
2. Department of Agriculture. Payroll and employee retirement system (Department of Accounting and General Services, Employees' Retirement System, Employee Union Trust Fund) information.
3. Department of Attorney General. Credit report (credit reporting agencies) information. Child support enforcement case (CSEA) information
4. Department of Budget and Finance. Personnel and employee retirement (Department of Accounting and General Services, Department of Human Resources Development, Department of Attorney General, lawyers, doctors) information. Employee health benefits (state agencies) information.
5. Department of Business Economic Development & Tourism. Contract information (contractors and vendors, Department of Attorney General). Security and background check (US Customs and Border Protection) information. Credit report (credit reporting agencies) information.
6. Department of Commerce and Consumer Affairs. Business and tax registration (licensing and law enforcement agencies, Department of Taxation) information. Producer license (National Association of Insurance Commissioners) information. Consumer protection case (law enforcement agencies) information.
7. Department of Defense. Employee and retirement system (Employer Union Trust Fund, Hawai'i Criminal Justice Data Center, Department of Human Services, FBI, loan companies) information.
8. Department of Education. Personnel and disability claim (Department of Labor and Industrial Relations) information. Retirement fund (Employees' Retirement System, Citistreet, AIG Valic) information.
9. Department of Health. Health care facility complaints and investigation (Department of Attorney General, Department of Human Services, Department of Taxation) information. Patient information (billing agency). Employment background check (adult protective services and child welfare services agencies) information. Client (Department of Human Services, Department of Education, providers) information.
10. Department of Human Resources Development. Employee payroll and life insurance plan (Department of Accounting and General Services, Life Insurance Company of the Southwest) information.
11. Department of Human Services. Case investigation (Department of Attorney General, FBI, District Court, physicians, employers) information. Employment verification information. Food stamp (USDA) and MedQuest (CMS) client information. Social services case (Social Security Administration, Department of Health, providers, pharmacies) information.
12. Department of Labor and Industrial Relations. Labor case (parties of interest) information. Personnel (employers, US Department of Labor) information. Disability Compensation and unemployment insurance case (parties of interest, National Child Support Agency, CSEA, US Department of Labor, Department of Taxation, Department of Human Services) information.
13. Department of Public Safety. Employee (Internal Revenue Service, Department of Taxation, Department of Attorney General, Judiciary, loan offices, landlords, employers)

information. Inmate (Internal Revenue Service, Social Security Administration, Department of Taxation, law enforcement agencies) information.

In addition to interagency document/record transmissions for employment and retirement related services, agencies report an expansive range of recurring personal information disclosures to federal and non-government entities including the Internal Revenue Service, credit reporting agencies, physicians, lawyers, Federal Bureau of Investigation, US Department of Agriculture, US Department of Health and Human Service, US Department of Labor, pharmacies).

Personal Information Disclosure Means

Again, notwithstanding the security measures deployed by agencies, the risks of unauthorized disclosures may be affected by the physical means deployed in the use/disclosure of personal information.

In the January 2007 personal information questionnaire, state and county agencies were queried regarding the means used to exchange/transmit personal information.

1. Telephone. Used by 65 of 75 (87%) responding agencies. Risks include breaches due to personal information being overheard by nearby individuals who are not authorized and personal information being requested over telephone by individuals not known and not verified by the agency as authorized to receive the information.
2. Interactive Voice Response (IVR) System. Only 11 of 75 (15%) of responding agencies report use of IVR systems. Risks include exposure of personal information to unauthorized individuals who illegally obtain account/PIN information to access the system.
3. Facsimile Machine. Used by 67 of 75 (89%) of responding agencies. Risks include exposure of personal information to unauthorized individuals in situations where facsimile machines are installed in shared office spaces and recipients are not pre-advised to expect the incoming fax transmission. Also, breaches may occur when faxes are inadvertently sent to a wrong fax number.
4. Email. Used by 65 of 75 (87%) of responding agencies. Risks include breaches by individuals who compromise email security systems to access email, individuals who use unsecured workstations to access email, and individuals who log in with a user ID/password obtained illegally to access email. Personal information breaches may also result when email is inadvertently sent to the wrong recipient.
5. Internet/Intranet Websites. Used by 46 of 75 (61%) of responding agencies. Risks include breaches by individuals who compromise website security protocols to access website content, individuals who log in with an active user ID/password obtained illegally to access website content, and application users who access website records containing personal information that they are not authorized to view. Also information breaches can result when personal information is inadvertently disclosed due to poor website design or in instances when agency websites permit public access to documents containing personal information.
6. Dialup/Broadband/Network File Transfer. Utilized by 32 of 75 (43%) of responding agencies. Risks include breaches by individuals who compromise security protocols to access data files during transmission and individuals who login with an active user ID/password obtained illegally.
7. Snail Mail. Used by 67 of 75 (89%) of responding agencies. Risks include breaches due to mail theft, when personal information is visible on/in an envelope, when mail is inadvertently sent to a wrong address and when mail is opened by an unauthorized individual.

8. Courier/Air Freight/Messenger Service. Used by 48 of 75 (64%) of responding agencies. Risks include breaches due to unauthorized access by carriers and due to package theft.

Physical and Technical Safeguards Deployed by Agencies

Risks to personal information breaches may be reduced by deploying physical and technical safeguards appropriate for defined security threat situations. In the January 2007 personal information questionnaire, state and county agencies were queried regarding the security safeguards used when transmitting documents/records containing personal information.

When transmitting information/documents in hard copy out of your unit, are there specific procedures applied for redacting or concealing personal information?

43 of 75 (57%) agencies responded in the affirmative. Safeguards reportedly deployed include envelopes are marked *Confidential*; document copies are made, personal information is redacted on the copy and then a photocopy of the redacted copy is made for transmission; and personal information is blacked out on documents.

Many agencies reported that personal information is not redacted since the information is required by law to support specified government processes, is required by an external entity, or due to resource limitations. A sample of agencies was further queried to obtain additional information on barriers to redacting personal information.

1. Department of Attorney General. Personal information is required to support debt collections performed for state agencies, criminal history management, child support enforcement, and fundraising professional management.

HRS Chapter 846D assigns responsibility to the department for the collection, storage, dissemination, and analysis of all juvenile justice custodial, adjudicative, and program data from all agencies which have primary investigative, action, or program responsibility for minors, including the county police departments, the county prosecutors, the family courts, and the Hawai'i youth correctional facilities, in such a manner as to balance the right of the public and press to be informed and the right of privacy and confidentiality of minors and their families, and to provide accurate, comprehensive, and timely information to government agencies concerned with juvenile offenders to carry out their responsibilities.

HRS § 576D-6(12)(B); § 576D-15(b), and § 576D-16(a) require that the SSN be submitted to the Child Support Enforcement Agency (CSEA).

HRS § 467B-12 requires registration including personal information by fundraising professions.

The department reports that redacting personal information would frustrate agency activities to perform mandated activities, render data in the Hawai'i Juvenile Justice Information System useless in violation with HRS 846D, violate HRS 467B, conflict with federal law and impede law enforcement research activities. Other barriers cited include reduced capacity to accurately match criminal records, potential liability if personal information is missed during redaction operations and manpower/resource limitations.

2. Department of Budget and Finance, Employees' Retirement System (ERS). Personal information is used/disclosed as part of employee retirement system activities.

Due to the high volume of documents/records, the ERS opts to redact only when records are disclosed outside of the agency. Barriers include concerns over liability when personal information is missed during redaction activities and dependency on SSN as a key index number. With regard the latter, ERS reports that there is resistance from external business partners to using an alternate member identification number.

3. Department of Commerce and Consumer Affairs. Personal information is used/disclosed to support business registration, securities registration/enforcement, and professional/vocational licensing activities.

The Business Registration Division reports a documents redaction project in progress costing approximately \$25,000 for extracting pdf files from an existing electronic documents repository, \$20,000 - \$30,000 for documents redaction, and \$20,000 - \$30,000 to reload documents.

Barriers cited to personal information redaction include the SSN is the primary index key used in the National Practitioners and NASD databases, potential record matching issues due to use of only the last four digits of the SSN and concerns over liability exposure when personal information is missed during redaction.

4. Department of Health, Vital Health Records. Manages birth, death, and marriage certificate processes.

Barriers cited include requirement to provide information to the Child Support Enforcement Agency (CSEA), Department of Human Services and county voter registration agencies.

5. Judiciary. Many laws, forms and court practices require use/disclosure of personal information. HRS § 571-84.5 and § 584-23.5 require that documents relating to child support matters include the SSN of any person who is a party to a divorce decree, or subject to a support order or paternity determination, or who made an acknowledgement of paternity. Many court documents containing personal information are considered public records and are accessible through the state website.

The Judiciary cites staff and financial resource limitations as barriers to redacting personal information used/maintained by the agency. The definition of personal information will significantly affect the scope of a proposed Judiciary redaction activity.

6. City and County of Honolulu, Department of Motor Vehicles. Personal information used/disclosed as part of motor vehicle and driver license management processes.

Barriers cited include concern over resource requirements to convert a mainframe based system to support role based user access controls and workload impacts resulting from increased public records disclosure requests once confidential information is redacted.

When personal information is transmitted electronically, are there technical safeguards (e.g. file encryption, SSL) used to protect the information from unauthorized access during transmission?

36 of 75 (48%) agencies responded in the affirmative. Considering the reported use/disclosure of personal information by email (73%) and Internet/intranet websites (52%), there are a substantial number of agencies with a relatively high risk of exposure to information breaches since no technical safeguards are being used when personal information is transmitted electronically.

When personal information is stored on portable computer devices (e.g. laptops, smart phones), and/or removable electronic data storage devices (e.g. floppy disks, CD-ROM, portable hard drives, USB drives) and is transported out of your unit facility, are any technical safeguards (e.g. passwords, encryption) used to protect the information from unauthorized access if the device is lost/stolen?

30 of 75 (40%) agencies responded in the affirmative. Some agencies reported that internal policies restrict users from storing personal information on portable devices. Notwithstanding such policies, the relatively low deployment rate of technical safeguards for these portable devices suggests that agencies are exposed to a high risk of information breaches. Among the technical safeguards reported by agencies are password protection to access files/portable devices and file/device encryption.

Business Associate Agreements

A critical component for managing the risk exposure to information breaches is assuring that there are adequate administrative safeguards put in place when agencies use third party entities to perform activities on their behalf where access to personal information is required. In the January 2007 personal information questionnaire, agencies were queried regarding their use of business associate agreements.

Does your unit have written agreements (contracts) with organizations that perform services on your behalf and have access to personal information?

Only 22 of 75 (29%) agencies responded in the affirmative. Agencies that reported that they use business associate agreements were further queried on specific provisions contained in their agreements.

Do the contracts/agreements with business associates contain language addressing:

1. *The allowed uses/disclosures of personal information and prohibited uses.* 17 of 22 (77%) agencies replied in the affirmative. An essential element of the agreement is clearly stating to the business associate what are the permissible uses/disclosures of personal information.
2. *Required physical/system safeguards to prevent unauthorized uses/disclosures.* 13 of 22 (59%) agencies responded in the affirmative. When personal information is transferred and/or transmitted from the agency to the business associate, there needs to be assurances that a level of technical and physical safeguards at least comparable to that deployed in the host agency is implemented to protect personal information from unauthorized disclosures.
3. *Required reporting in the event of unauthorized use/disclosure and/or security breaches.* 10 of 22 (46%) agencies responded in the affirmative. Hawai'i agencies are required to provide notification to individuals regarding security breaches involving personal information. This requirement applies even in instances where the security breach occurs while personal information is temporarily in the custody of a business associate.
4. *Requirements to assure that agents/subcontractors to whom personal information is disclosed agree to the same conditions.* 8 of 22 (38%) agencies responded in the affirmative. If the business associate uses a subcontractor to perform work, there needs to be assurances that requirements to safeguard personal information are also observed by the subcontractor.
5. *Requirements to return or appropriately dispose/destroy personal information at the conclusion of the contract.* 11 of 22 (50%) agencies responded in the affirmative. There needs to be assurances that no personal information remains with the business associate after the conclusion of the contracted work.

Administrative Safeguards

Administrative safeguards are an essential component of the security framework to protect personal information from unauthorized use/disclosures. These include implementation of and workforce training on agency policies/procedures/standards designed to protect personal information. Ideally, these administrative safeguards should be deployed at least department-wide when personal information is commonly transmitted between department units.

In the January 2007 personal information questionnaire, agencies were queried on the workforce policies and agency policies/procedures deployed to protect personal information.

Are there policies on workforce member use, handling and disclosure of personal information? 59 of 75 (79%) agencies responded in the affirmative. Minimally, to assure compliance with HRS Chapters 487J, 487N, and 487R, all agencies should have a policy on the permissible

use/disclosure of personal information that applies to agency personnel, volunteers, researchers, contractors/vendors and business associates.

Some responding agencies state that they have unwritten/oral policies that are communicated to staff. However, unwritten policies are generally regarded as insufficient since they may not be communicated consistently to all staff members, all staff members may not receive the policy communication, there may be confusion when policies are updated/modified and it may be difficult to apply sanctions in situations when policies are violated.

Do workforce members sign confidentiality agreements applicable to personal information that they may use/disclose as part of their job function? Only 19 of 75 (25%) agencies replied in the affirmative. Confidentiality agreements are useful tools for emphasizing agency commitments to protect personal information and to remind workforce members of their affirmative responsibilities in this regard. They also can serve as evidence in disciplinary hearings when staff policy violations result in information breaches.

Are there policies/procedures to assure that workforce members access to personal information is terminated (e.g. return of keys, access entry combinations changed, passwords deactivated) when the workforce member separates/terminates from employment? 58 of 75 (77%) agencies responded in the affirmative. These policies minimize the risk that terminated employees can gain access to personal information after they have separated from employment at the agency.

Is training on the appropriate use/disclosure of personal information required for workforce members? 21 of 75 (24%) agencies responded in the affirmative. Implementing department-wide training on the appropriate use/disclosure of personal information assures that staff have general awareness and can act appropriately to protect personal information that they use/maintain as part of their job responsibilities.

Are there general policies or procedures about the appropriate and restricted handling, use, and disclosure of personal information? 51 of 75 (68%) agencies responded in the affirmative. Agencies that responded NO either stated that they had no policies or that they had unwritten policies understood by staff.

Are there policies or procedures requiring that personal information is secured and that stipulate the manner that is used to safeguard the information? 49 of 75 (65%) responded in the affirmative. Among the safeguards cited by agencies:

1. Department of Accounting and General Services. Have written policies on SSN use/disclosure and confidential information disposal.
2. Department of Agriculture. No department-wide guidance offered. Animal Industries Division cites a policy requiring a written notarized document authorizing release of personal information.
3. Department of Budget and Finance. Cites the Policy and Procedures on Safekeeping and Proper Destruction of Personal Information and Security Breach Notifications.
4. Department of Commerce and Consumer Affairs. Cites policies to secure confidential information on computer systems, password guidelines and laptop usage.
5. Department of Defense. Cites Department of Human Resource Development P&P 701.001 relating to policies on personnel files.
6. Department of Hawaiian Home Lands. Cites UIPA Opinion Letter 89-4 and 91-19 on redaction. Also lists guidance on restricting copies of personal information on laptops and USB devices.
7. Department of Health. Cites HIPAA policies.
8. Department of Human Resources Development. Cites Official Personnel Folders Policy & Procedures 701.001 and Acceptable Usage of Information Technology Resources Policy & Procedures No. 103.001.

Are there policies or procedures for restricting the use/disclosure of personal information to a need to know basis? 48 of 75 (64%) agencies responded in the affirmative. These policies affirm the obligation to use only the minimum information necessary to perform one's job responsibilities and restrictions to not disclose personal information to individuals who are not authorized.

Are there policies or procedures to verify the identity of individuals requesting access to personal information, if they are not known? 28 of 75 (37%) agencies responded in the affirmative. Under HRS Chapter 92F, agency records containing personal information are generally regarded to be confidential. However, HRS Chapter 92F stipulates that agencies implement specified processes to provide access to individuals to records containing their personal information. For those situations, a best practice is the policy to verify the identity of individuals, particularly if access requests are not made in person.

Are there policies or procedures that stipulate the conditions for secure storage/retention of personal information? 50 of 75 (67%) agencies responded in the affirmative. Among policies cited are:

1. Department of Agriculture. Animal Industries Division cites policies requiring that documents containing personal information be marked Confidential and that records containing personal information shall be secured in locked rooms and/or locked in file cabinets when not in use.
2. Department of Budget and Finance. Cites the Policy and Procedures on Safekeeping and Proper Destruction of Personal Information and Security Breach Notifications.
3. Department of Commerce and Consumer Affairs. Cites policy to secure confidential information on computer systems.
4. Department of Defense. Refers to Department of Human Resources Development P&P 701.000 regarding personnel files.
5. Department of Hawaiian Home Lands. Cites the Central File Room Procedure. Also states that there is a check-in/check-out system with tracking capabilities for applicant/lessee files.
6. Department of Human Resources Development. Cites Official Personnel Folders Policy & Procedures 701.001.

Are there policies or procedures that stipulate the conditions for secure disposal of personal information? 55 of 75 (73%) agencies responded in the affirmative. Implementation of these policies will assure agency capabilities to comply with HRS Chapter 487R (Destruction of Personal Information Records).

Are there policies or procedures that support the capability to identify personal information records contained in data/document files that are stored on portable computer and data storage devices in case they are lost/stolen? Only 19 of 75 (25%) agencies responded in the affirmative. These policies would assure agencies have the capability to determine what individuals are affected by the loss of portable computer or data storage devices containing personal information. HRS Chapter 487N requires that individual be notified in cases of security breaches when there is a reasonable probability of identity theft.

Section 6. Identity Theft Task Force Recommendations

Decrease Unnecessary Use of Personal Information

A critical means to reduce exposure to identity theft is to limit the unnecessary use of personal information and to encourage agencies to develop alternative strategies for identity management. Accordingly, the Identity Theft Task Force recommends:

Recommendation No. 1. Require Annual Report on Systems that Use Personal Information

Effective January 1, 2009, State and County agencies shall file an annual report with the Information Privacy and Security Workgroup (described in a later recommendation) on the existence and character of each system added or eliminated since the last report. Among the required elements of the annual report are a description of personal information systems, justification for the system, the categories of personal information held, and the job classifications of agency personnel who have access.

The annual report requirement accomplishes several objectives:

1. Enables legislative oversight over personal information collection by agencies and facilitates actions to prevent potential unnecessary intrusion on citizen privacy rights.
2. Facilitates agency information planning processes and offers opportunities to reduce redundant/excessive collection of personal information.
3. Provides basic inventory of personal information systems at agencies that may facilitate investigations in cases of security breaches.

Recommendation No. 2. Limit the Personal Information in Agency Records

By September 30, 2008, all government agencies that collect, maintain, and disseminate records containing personal information subject to HRS §92F-12 disclosure, shall develop a plan to protect and redact personal information (specifically social security numbers) contained in existing, hardcopy records before these records are made available for public inspection. Proposed budgets to protect and redact personal information contained in existing, hardcopy records shall be prepared for submittal as part of the Executive, Judiciary and Legislative budgets by December 31, 2008.

Agencies failing to develop a plan by the compliance date shall be required to implement procedures to provide for an accounting of records containing social security numbers disclosed pursuant HRS §92F-12. The accounting of disclosures shall include the date, nature, and purpose of each disclosure of a record and the name and address of the person to whom the disclosure is made. An accounting shall not be required when the disclosure is made to the individual about whom the record pertains. Agencies shall retain the accounting for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made and shall make the accounting available to the individual named in the record at his/her request.

By December 1, 2008, implement legislation that directs State and County agencies to limit the personal information that is maintained in agency records to that which is relevant and necessary to accomplish a purpose of the agency required or authorized by Hawaii statutes, Hawaii administrative rules, or mandated by the federal government.

Further, agencies shall be directed to collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source.

These recommendations have several purposes:

1. Compels agency management to inventory current holdings of personal information and to assess the scope/justification for these systems against designated agency functions.
2. Presents agency management with the opportunity to reduce the collection and retention of personal information in areas where it is found to be excessive for the agency function supported.
3. Directing agencies to collect personal information directly from individuals offers two benefits. One, it provides the individuals with some control over the information that they give to agencies. And two, it serves to minimize the propagation of personal information collections by agencies.

Recommendation No. 3. Reduce Use of Social Security Numbers

State and County agencies shall review their use of social security numbers in agency systems/programs to identify instances in which collection or use of the social security number is superfluous.

By December 1, 2008, all government agencies that collect, maintain and disseminate records pursuant HRS §92F-12 and that contain personal information shall develop a plan to eliminate the unnecessary collection and use of social security numbers.

Recommended elements for agency plans include collecting social security numbers preferably only where required to do so by federal or state law; when collecting social security numbers is allowed, by law, proceed as reasonably necessary for the proper administration of lawful agency business; and for instances when a unique identifier is required, develop alternatives to using the social security number.

Agencies shall submit their plans to the Information Privacy and Security Workgroup for review and comment. Funding requests associated with plans to eliminate the unnecessary use of social security numbers shall be prepared for submittal to the 2009 Legislature.

This recommendation parallels to some degree the recommendation above pertaining to limiting the use of personal information. The focus on social security number in this recommendation is because of the greater exposure to financial damage and the difficulty to mitigate the harmful effects of security breaches involving social security numbers.

Implement Safeguards to Protect Personal Information

A significant finding of the Identity Theft Task Force research is the absence of comprehensive administrative, technical and physical safeguards deployed at State and County agencies covering the privacy and security of personal information in paper and electronic based records. Where they exist, the safeguards appear to be system and/or agency specific and not applicable department-wide. And they do not appear to apply systematically to the use/disclosure of personal information with outside agencies and third parties.

Addressing this deficiency will require a government-wide effort that will likely span a number of years and require significant financial resources. The Identity Theft Task Force has determined that actions in the following areas may result in improved short term security for personal information used by agencies:

Recommendation No. 4. Require State and County Agencies to Assign Policy and Oversight Responsibilities

By September 1, 2008, each State and County agency shall assign policy and oversight responsibilities for the protection of personal information. The named department/agency unit shall:

1. Coordinate agency compliance with the requirements of HRS Chapter 487J (Social Security Number Protection), HRS Chapter 487N (Notice of Security Breach), and HRS Chapter 487R (Destruction of Personal Information Records).
2. Assist individuals with identity theft and other privacy-related concerns.
3. Provide education and information to agency staff on privacy and security issues.
4. Coordinate with local, state, and federal law enforcement on identity theft investigations.
5. Recommend policies and practices that protect individual privacy rights.

This recommendation implements a security best practice by assigning specific responsibilities for managing the privacy and security of personal information used by agencies. Currently, most State and County agency have not made specific privacy/security responsibility assignments as it may pertain to paper and electronic based records.

Recommendation No. 5. Issue Guidance on Use of Personal Information in Human Resources Functions

By January 1, 2009, the lead agencies responsible for human resources functions at the State and respective County governments shall issue guidance on recommended practices to minimize unauthorized access to personal information pertaining to personnel recruitment, background checks, testing; employee retirement and health benefits; and time reporting and payroll.

A significant proportion of the personal information that is used and transmitted by agencies is directly related to support of human resources functions. Directing the lead human resources agencies to issue guidance on recommended safeguards can reduce the exposure to security breaches in these critical agency processes. Suggested areas for attention include:

1. Physical security standards for paper and electronic records that are stored onsite and offsite and for removable storage media (e.g. laptops, USB storage devices, CD, tapes).
2. Administrative safeguards to control and monitor access to human resources information systems.
3. Technical safeguards to assure the confidentiality and integrity of information transmitted over networks and stored on laptop computers and removable storage devices.

Recommendation No. 6. Require State and County Agencies to Use Third Party Information Use Agreements

By September 1, 2008, each State and County agency shall include provisions in all new and renewing contracts with third parties, providing support services on behalf of the agency, that include the use/disclosure of personal information administered by the agency. Required elements in the agreements shall include:

1. Implementation of technical safeguards acceptable to the agency to reduce exposure to unauthorized access to personal information.
2. Mandatory training of third party staff on security awareness topics.
3. Confidentiality agreements signed by staff that acknowledge that the agency personal information is confidential and that access to the information is restricted to minimum necessary and to uses consistent with the contracted services.
4. No personal information shall be retained or repurposed (e.g. used for a purpose other than that for which it was originally collected) by the third party and all copies of personal information records shall be destroyed at the conclusion of the contract.
5. Provide prompt and complete disclosure of security breaches.
6. Provide complete log of disclosures made by staff of agency personal information.

This recommendation provides agencies with assurances that acceptable administrative, physical, and technical safeguards are deployed by third party entities to protect the personal information obtained from the agency. It also assures appropriate notification to agencies in case of security breaches and/or disclosures of personal information by the third party entity.

Ensure Effective, Risk-Based Responses to Data Breaches

According to the Government Accounting Office (GAO), *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However the Full Extent is Unknown*, June 2007, the extent to which data breaches have resulted in identity theft is not well known. Requiring notification to affected individuals in cases of breaches has obvious benefits such as allowing individuals the opportunity to take measures to mitigate potential harm. However, there are considerable expenses associated with performing notifications and there is a danger that expansive requirements to provide notices may cause individuals to ignore the notices.

The Identity Theft Task Force has developed the following recommendations for implementing standardized, risk-based notification processes in cases of security breaches:

Recommendation No. 7. Issue Data Breach Guidance to Agencies

By September 1, 2008, the Governor shall appoint an Information Privacy and Security Workgroup composed of selected State and County agency staff. The Workgroup shall be administratively attached to a State Executive Branch department and supported by three staff analyst positions.

The Workgroup shall develop and formally approve a set of guidelines that sets forth the factors that should be considered in deciding whether, how, and when to inform affected individuals of the loss of personal information that can contribute to identity theft. The

Workgroup shall also review the annual reports submitted by State and County agencies and submit a summary report to the Legislature on its findings, significant trends, and recommendations to assure the protection of personal information used by agencies.

This recommendation addresses several concerns:

1. Provides a unified State and County standard for determining when to notify individuals of a security breach.
2. Recognizes that not all security breaches may result in identity theft and that the collateral damage/cost of providing notification may exceed the benefit of providing the notice to individuals.
3. Reduces the resources that may be required by individual agencies to develop notification processes in compliance with HRS Chapter 487N.

Recommendation No. 8. Require Agencies to Develop and Implement a Breach Notification Policy

By September 1, 2008, all State/County agencies shall develop a breach notification policy and ensure that proper safeguards are in place to protect personal information. The scope of the policy shall apply to both electronic systems and paper documents. Six (6) elements shall be addressed in the policy when considering external notification: 1) whether breach notification is required; 2) timeliness of the notification; 3) source of the notification, 4) contents of the notification; 5) means of providing the notification; 6) who receives notification.

Agencies shall submit their breach notification policies for review and comment by their respective Deputy Attorney General/Corporation Counsel and shall amend their policies to address recommendations/issues cited by legal counsel. Further, agencies shall review their breach notification policies on an annual basis and update them as necessary. Should there be material changes to the policy, appropriate notice shall be disseminated to agency staff.

This recommendation has the following benefits:

1. Addresses the finding that not all agencies have developed formal policies and procedures to comply with HRS Chapter 487N. Without such guidance in place, it is unlikely that agencies will be able to appropriately comply with requirements to report breaches to the Legislature and law enforcement, as necessary.
2. Facilitates integration of internal security breach response processes with the guidelines developed by the Information Privacy and Security Workgroup for risk-based notification to affected individuals

Recommendation No. 9. Assess and Recommend Initiatives to Mitigate the Impact of Identity Theft on Individuals

By January 1, 2009, the Information Privacy and Security Workgroup shall submit to the Legislature an assessment and recommendations on initiatives to mitigate the negative impacts of identity theft incidents on individuals. Emphasis shall be placed on assessing the merits of identity theft passport and identity theft registry initiatives as implemented in other state jurisdictions. With some state variations, these initiatives provide means to inform law enforcement agencies that a person of interest is an identity theft victim and that a mistaken criminal history may have been created in that individual's name.

Educate Agencies on How to Protect Data

To ensure that government agencies receive specific guidance on concrete steps that they can take to improve their personal information security measures, the Identity Theft Task Force recommends:

Recommendation No. 10. Develop Concrete Guidance and Best Practices

By March 31, 2009, the Governor appointed Information Privacy and Security Workgroup shall identify best practices in the areas of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs.

By July 31, 2009, the products of the Workgroup should be posted on respective State/County websites so that it is readily accessible by agency personnel.

A finding of the Task Force is that there does not appear to be standard guidance offered to State or County agencies on best practices regarding administrative and technical safeguards to protect personal information. This recommendation would provide a short-term remedy until a more comprehensive information security and security awareness training program can be developed.

Recommendation No. 11. Issue Portable Storage and Communication Devices Guidance to Agencies

By December 31, 2008, the Information Privacy and Security Workgroup, with staff support from the Department of Accounting and General Services, Information and Communications Services Division shall issue guidance to the information technology managers in all State agencies on their responsibilities to protect laptops, removable data storage devices and communication devices used to remotely access applications installed on the State network. The guidance shall include recommendations on best practices and standards for protecting personal information that may be used/stored/transmitted with these devices. The lead information technology managers in the respective counties shall issue similar guidance to the county agencies.

The research performed by the Identity Theft Task Force suggests that laptop computers and removable data storage devices are factors in many security breaches of personal information. This recommendation addresses this significant area of vulnerability.

Revise the Effective Date of Required Social Security Number Protection Measures

To provide government agencies with the opportunity to request appropriate resources to support implementation activities related to complying with HRS Chapter 487J, the Identity Task Force recommends:

Recommendation No. 12. Revise the Effective Date for Act 137, Session Laws of Hawaii 2006 to July 1, 2009.

Recommendation No. 2 directs state and county agencies to submit budget proposals to fund compliance activities related to HRS Chapter 487J by December 31, 2008. Inasmuch as the scheduled date for complying with HRS Chapter 487J is July 1, 2008, revising the effective date to July 1, 2009 will provide the government agencies with additional time to apply approved funding to implement compliance activities. The revised effective date will be applicable to businesses as well as government agencies.

This page intentionally left blank

Appendix 1. Personal Information Definitions

State	Identity Theft	Security Breach
Alabama	<p>13A-8-191. Identifying Information.</p> <p>Any information, used either alone or in conjunction with other information, that specifically identifies a person or a person's property, and includes, but is not limited to, any of the following information related to a person:</p> <ul style="list-style-type: none"> a. Name. b. Date of birth. c. Social Security number. d. Driver's license number. e. Financial services account numbers, including checking and savings accounts. f. Credit or debit card numbers. g. Personal identification numbers (PIN). h. Electronic identification codes. i. Automated or electronic signatures. j. Biometric data. k. Fingerprints. l. Passwords. m. Parent's legal surname prior to marriage. n. Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services. 	
Alaska	<p>Sec. 40.25.350(2). Personal information</p> <p>Means information that can be used to identify a person and from which judgments can be made about a person's character, habits, avocations, finances, occupation, general reputation, credit, health, or other personal characteristics, but does not include a person's name, address, or telephone number, if the number is published in a current telephone directory, or information describing a public job held by a person.</p>	

State	Identity Theft	Security Breach
Arizona	<p>Sec. 13-2001. Personal identifying information</p> <p>Means any written document or electronic data that does or purports to provide information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number, photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information.</p>	<p>Sec. 44-7501</p> <p>Individual's first name or first initial and last name in combination with any of the following unencrypted, unredacted or nonsecured information:</p> <ol style="list-style-type: none"> a. The individual's social security number b. The individual's driver license or nonoperating identification license number. c. The individual's financial account number or credit or debit card number in combination with any required security code that would permit access to the individual's financial account.
Arkansas	<p>5-37-227. "Identifying information" includes, but is not limited to, a:</p> <ol style="list-style-type: none"> (A) Social security number; (B) Driver's license number; (C) Checking account number; (D) Savings account number; (E) Credit card number; (F) Debit card number; (G) Personal identification number; (H) Electronic identification number; (I) Digital signature; or (J) Any other number or information that can be used to access a person's financial resources; 	<p>4-110-103. "Personal information"</p> <p>Means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted:</p> <ol style="list-style-type: none"> (A) Social security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, 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; and (D) Medical information
California	<p>530.55. "Personal identifying information"</p> <p>Means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number</p>	<p>1798.82. "Personal information"</p> <p>Means 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:</p> <ol style="list-style-type: none"> (1) Social security number. (2) Driver's license number or California Identification Card number. (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.

State	Identity Theft	Security Breach
	of an individual person, or an equivalent form of identification.	
Colorado	<p>18-5-901. "Personal identifying information"</p> <p>Means information that may be used, alone or in conjunction with any other information, to identify a specific individual, including but not limited to a name; a date of birth; a social security number; a password; a pass code; an official, government-issued driver's license or identification card number; a government passport number; biometric data; or an employer, student, or military identification number.</p>	<p>6-1-716. "Personal information"</p> <p>Means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:</p> <p>(A) Social security number;</p> <p>(B) Driver's license number or identification card number;</p> <p>(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.</p>
Connecticut	<p>53a-129a. "Personal identifying information"</p> <p>Means any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual including, but not limited to, such individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation.</p>	<p>Sec. 36a-701b. "Personal information"</p> <p>Means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (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 publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.</p>

State	Identity Theft	Security Breach
Delaware	<p>§ 854. "Personal identifying information"</p> <p>Includes name, address, birth date, Social Security number, driver's license number, telephone number, financial services account number, savings account number, checking account number, credit card number, debit card number, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-mail address, computer system password, mother's maiden name or similar personal number, record or information</p>	<p>Chapter 12B "Personal information"</p> <p>Means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:</p> <ul style="list-style-type: none"> a. Social Security number; b. Driver's license number or Delaware Identification Card number; or c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. <p>The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records</p>
District of Columbia	<p>D.C. Code 22-3227.01. "Personal identifying information"</p> <p>Includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> (A) Name, address, telephone number, date of birth, or mother's maiden name. (B) Driver's license or driver's license number, or non-driver's license or non-driver's license number; (C) Savings, checking, or other financial account number; (D) Social security number or tax identification number; (E) Passport or passport number; (F) Citizenship status, visa, or alien registration card or number; (G) Birth certificate or a facsimile of a birth certificate (H) Credit or debit card, or credit or debit card number (I) Credit history or credit rating (J) Signature; (K) Personal identification number, electronic identification number, password, access code or device, electronic address, electronic identification number, routing information or code, digital signature, or telecommunication identifying information; (L) Biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (M) Place of employment, employment history, or employee identification number; and (N) Any other numbers or information that can 	

State	Identity Theft	Security Breach
	<p>be used to access a person's financial resources, access medical information, obtain identification, act as identification, or obtain property.</p>	
<p>Florida</p>	<p>817.568 "Personal identification information"</p> <p>Means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:</p> <ol style="list-style-type: none"> 1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card; 2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; 3. Unique electronic identification number, address, or routing code; 4. Medical records; 5. Telecommunication identifying information or access device; or 6. Other number or information that can be used to access a person's financial resources. 	<p>817.5681 "Personal information"</p> <p>Means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:</p> <ol style="list-style-type: none"> (a) Social security number. (b) Driver's license number or Florida Identification Card number. (c) Account number, credit card number, 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. <p>For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.</p>
<p>Georgia</p>	<p>§ 16-9-120 "Identifying information"</p> <p>Shall include, but not be limited to:</p> <ol style="list-style-type: none"> (A) Current or former names; (B) Social security numbers; (C) Driver's license numbers; (D) Checking account numbers; (E) Savings account numbers; (F) Credit and other financial transaction card numbers; (G) Debit card numbers; (H) Personal identification numbers; (I) Electronic identification numbers; (J) Digital or electronic signatures; (K) Medical identification numbers; (L) Birth dates; 	<p>§ 10-1-911. "Personal information"</p> <p>Means 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 or redacted:</p> <ol style="list-style-type: none"> (A) Social security number; (B) Driver's license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform

State	Identity Theft	Security Breach
	<p>(M) Mother's maiden name;</p> <p>(N) Selected personal identification numbers;</p> <p>(O) Tax identification numbers;</p> <p>(P) State identification card numbers issued by state departments; or</p> <p>(Q) Any other numbers or information which can be used to access a person's or entity's resources.</p>	<p>identity theft against the person whose information was compromised.</p>
Hawaii	<p>§708-800. "Personal information"</p> <p>Means information associated with an actual person or a fictitious person that is a name, an address, a telephone number, an electronic mail address, a driver's license number, a social security number, an employer, a place of employment, information related to employment, an employee identification number, a mother's maiden name, an identifying number of a depository account, a bank account number, a password used for accessing information, or any other name, number, or code that is used, alone or in conjunction with other information, to confirm the identity of an actual or a fictitious person.</p>	<p>§487N-1. "Personal information"</p> <p>Means 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:</p> <p>(1) Social security number;</p> <p>(2) Driver's license number or Hawaii identification card number; or</p> <p>(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.</p>
Idaho	<p>18-3122. "Personal identifying information"</p> <p>Means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, checking account number, savings account number, financial transaction card number, or personal identification code of an individual person, or any other numbers or information which can be used to access a person's financial resources.</p>	<p>28-51-105. "Personal information"</p> <p>Means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:</p> <p>(a) Social security number;</p> <p>(b) Driver's license number or Idaho identification card number; or</p> <p>(c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.</p> <p>The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.</p>

State	Identity Theft	Security Breach
Illinois	<p>720 ILCS 5/16G□10. "Personal identifying information"</p> <p>Means any of the following information:</p> <ul style="list-style-type: none"> (1) A person's name; (2) A person's address; (2.5) A person's date of birth; (3) A person's telephone number; (4) A person's drivers license number or State of Illinois identification card as assigned by the Secretary of State of the State of Illinois or a similar agency of another state; (5) A person's Social Security number; (6) A person's public, private, or government employer, place of employment, or employment identification number; (7) The maiden name of a person's mother; (8) The number assigned to a person's depository account, savings account, or brokerage account; (9) The number assigned to a person's credit or debit card, commonly known as a "Visa Card", "Master Card", "American Express Card", "Discover Card", or other similar cards whether issued by a financial institution, corporation, or business entity; (10) Personal identification numbers; (11) Electronic identification numbers; (12) Digital signals; (12.5) User names, passwords, and any other word, number, character or combination of the same usable in whole or part to access information relating to a specific individual, or to the actions taken, communications made or received, or other activities or transactions of a specific individual. (13) Any other numbers or information which can be used to access a person's financial resources, or to identify a specific individual, or the actions taken, communications made or received, or other activities or transactions of a specific individual. 	<p>(815 ILCS 530/5) Sec. 5. Personal information"</p> <p>Means 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 or redacted:</p> <ul style="list-style-type: none"> (1) Social Security number. (2) Driver's license number or State identification card number. (3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

State	Identity Theft	Security Breach
Indiana	<p>IC 35-43-5-1. "Identifying information"</p> <p>Means information that identifies an individual, including an individual's:</p> <p>(1) name, address, date of birth, place of employment, employer identification number, mother's maiden name, Social Security number, or any identification number issued by a governmental entity;</p> <p>(2) unique biometric data, including the individual's fingerprint, voice print, or retina or iris image;</p> <p>(3) unique electronic identification number, address, or routing code;</p> <p>(4) telecommunication identifying information; or</p> <p>(5) telecommunication access device, including a card, a plate, a code, a telephone number, an account number, a personal identification number, an electronic serial number, a mobile identification number, or another telecommunications service or device or means of account access that may be used to:</p> <p>(A) obtain money, goods, services, or any other thing of value; or</p> <p>(B) initiate a transfer of funds.</p>	<p>IC 24-4.9-2-10 "Personal information"</p> <p>Means:</p> <p>(1) a Social Security number that is not encrypted or redacted; or</p> <p>(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:</p> <p>(A) A driver's license number.</p> <p>(B) A state identification card number.</p> <p>(C) A credit card number.</p> <p>(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.</p> <p>The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.</p>
Iowa	<p>715A.8 "identification information"</p> <p>Includes, but is not limited to, the name, address, date of birth, telephone number, driver's license number, nonoperator's identification card number, social security number, student identification number, military identification number, alien identification or citizenship status number, employer identification number, signature, electronic mail signature, electronic identifier or screen name, biometric identifier, genetic identification information, access device, logo, symbol, trademark, place of employment, employee identification number, parent's legal surname prior to marriage, demand deposit account number, savings or checking account number, or credit card number of a person.</p>	

State	Identity Theft	Security Breach
Kansas	<p>21-3830. "identification document"</p> <p>Means any card, certificate or document or banking instrument including, but not limited to, credit or debit card, which identifies or purports to identify the bearer of such document, whether or not intended for use as identification, and includes, but is not limited to, documents purporting to be drivers' licenses, nondrivers' identification cards, certified copies of birth, death, marriage and divorce certificates, social security cards and employee identification cards.</p>	
Kentucky	<p>514.160 "Identifying information"</p> <p>- name, address, telephone number, electronic mail address, Social Security number, driver's license number, birth date, personal identification number or code, and any other information which could be used to identify the person, including unique biometric data.</p>	
Louisiana	<p>§67.16. "Personal identifying information"</p> <p>Shall include but not be limited to an individual's:</p> <ul style="list-style-type: none"> (a) Social security number. (b) Driver's license number. (c) Checking account number. (d) Savings account number. (e) Credit card number. (f) Debit card number. (g) Electronic identification number. (h) Digital signatures. (i) Birth certificate. (j) Date of birth. (k) Mother's maiden name. (l) Armed forces identification number. (m) Government issued identification number. (n) Financial institution account number. 	<p>RS 51:3073. "Personal information"</p> <p>Means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:</p> <ul style="list-style-type: none"> (i) Social security number. (ii) Driver's license number. (iii) 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. <p>"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>
Maine	<p>Title 17-A: Maine Criminal Code, Part 2: Substantive Offenses, Chapter 37: Fraud, §905-A. "legal identification"</p> <p>Includes a social security card, social security number, birth certificate, driver's license, government-issued identification card, oral statement of full name and date of birth or any other means of identifying a person that is generally accepted as accurate and reliable</p>	

State	Identity Theft	Security Breach
Maryland	<p>8-301. "Personal identifying information"</p> <p>Means a name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, mother's maiden name, bank or other financial institution account number, date of birth, personal identification number, credit card number, or other payment device number</p>	
Massachusetts	<p>Chapter 266: Section 37E. "Personal identifying information"</p> <p>Any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.</p>	
Michigan	<p>445.63 Identity "Personal identifying information"</p> <p>Means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.</p>	<p>445.63 "Personal information"</p> <p>Means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:</p> <ul style="list-style-type: none"> (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

State	Identity Theft	Security Breach
Minnesota	<p>609.527 "Identity"</p> <p>Means any name, number, or data transmission that may be used, alone or in conjunction with any other information, to identify a specific individual or entity, including any of the following:</p> <p>(1) a name, Social Security number, date of birth, official government-issued driver's license or identification number, government passport number, or employer or taxpayer identification number;</p> <p>(2) unique electronic identification number, address, account number, or routing code; or</p> <p>(3) telecommunication identification information or access device.</p>	<p>325E.61 "Personal information"</p> <p>Means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:</p> <p>(1) Social Security number;</p> <p>(2) driver's license number or Minnesota identification card number; or</p> <p>(3) account number or 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.</p>
Missouri	<p>570.223. 1. "means of identification"</p> <p>Includes, but is not limited to, the following:</p> <p>(1) Social Security numbers;</p> <p>(2) Drivers license numbers;</p> <p>(3) Checking account numbers;</p> <p>(4) Savings account numbers;</p> <p>(5) Credit card numbers;</p> <p>(6) Debit card numbers;</p> <p>(7) Personal identification (PIN) code;</p> <p>(8) Electronic identification numbers;</p> <p>(9) Digital signatures;</p> <p>(10) Any other numbers or information that can be used to access a person's financial resources;</p> <p>(11) Biometric data;</p> <p>(12) Fingerprints;</p> <p>(13) Passwords;</p> <p>(14) Parent's legal surname prior to marriage;</p> <p>(15) Passports; or</p> <p>(16) Birth certificates.</p>	

State	Identity Theft	Security Breach
Montana	<p>45-6-332. "Personal identifying information"</p> <p>Includes but is not limited to the name, date of birth, address, telephone number, driver's license number, social security number or other federal government identification number, place of employment, employee identification number, mother's maiden name, financial institution account number, credit card number, or similar identifying information relating to a person.</p>	
Nebraska	<p>Section 28-608. Personal identifying information</p> <p>Means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person including a person's: (i) Name; (ii) date of birth; (iii) address; (iv) motor vehicle operator's license number or state identification card number as assigned by the State of Nebraska or another state; (v) social security number or visa work permit number; (vi) public, private, or government employer, place of employment, or employment identification number; (vii) maiden name of a person's mother; (viii) number assigned to a person's credit card, charge card, or debit card, whether issued by a financial institution, corporation, or other business entity; (ix) number assigned to a person's depository account, savings account, or brokerage account; (x) personal identification number as defined in section 8-157.01; (xi) electronic identification number, address, or routing code used to access financial information; (xii) digital signature; (xiii) telecommunications identifying information or access device; (xiv) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; and (xv) other number or information which can be used to access a person's financial resources</p>	<p>Section 87-802. Personal information</p> <p>Means a Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:</p> <p>(a) Social security number;</p> <p>(b) Motor vehicle operator's license number or state identification card number;</p> <p>(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;</p> <p>(d) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or</p> <p>(e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.</p>
Nevada	<p>NRS 205.4617 " Personal identifying information"</p> <p>1. Except as otherwise provided in subsection 2, "personal identifying information" means any information designed, commonly used or capable of being used, alone or in conjunction with any other information, to identify a living or deceased person, including, without limitation:</p> <p>(a) The current or former name, driver's license number, identification card number, social security number, checking account number, savings account number, credit card number, debit card number, financial services account number, date of birth, place of employment and maiden name of the mother of a person.</p> <p>(b) The unique biometric data of a person, including, without limitation, the fingerprints, facial scan identifiers, voiceprint, retina image and iris image of a person.</p>	<p>NRS 603A.040 Personal Information"</p> <p>Means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:</p> <p>1. Social security number.</p> <p>2. Driver's license number or identification card number.</p> <p>3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.</p>

State	Identity Theft	Security Breach
	<p>(c) The electronic signature, unique electronic identification number, address or routing code, telecommunication identifying information or access device of a person.</p> <p>(d) The personal identification number or password of a person.</p> <p>(e) The alien registration number, government passport number, employer identification number, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number or health insurance identification number of a person.</p> <p>(f) The number of any professional, occupational, recreational or governmental license, certificate, permit or membership of a person.</p> <p>(g) The number, code or other identifying information of a person who receives medical treatment as part of a confidential clinical trial or study, who participates in a confidential clinical trial or study involving the use of prescription drugs or who participates in any other confidential medical, psychological or behavioral experiment, study or trial.</p> <p>(h) The utility account number of a person.</p> <p>2. To the extent that any information listed in subsection 1 is designed, commonly used or capable of being used, alone or in conjunction with any other information, to identify an artificial person, "personal identifying information" includes information pertaining to an artificial person.</p>	
New Hampshire	<p>638:25. "Personal identifying information"</p> <p>Means any name, number, or information that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, employer or place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number, debit card number, personal identification number, account number, or computer password identification.</p>	

State	Identity Theft	Security Breach
New Jersey	<p>2C:20-1. "Personal identifying information"</p> <p>Means any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual and includes, but is not limited to, the name, address, telephone number, date of birth, social security number, official State issued identification number, employer or taxpayer number, place of employment, employee identification number, demand deposit account number, savings account number, credit card number, mother's maiden name, unique biometric data, such as fingerprint, voice print, retina or iris image or other unique physical representation, or unique electronic identification number, address or routing code of the individual.</p>	<p>C.56:8-161 Personal information"</p> <p>Means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or 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. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.</p>
New Mexico	<p>30-16-24-1. "personal identifying information"</p> <p>Means information that alone or in conjunction with other information identifies a person, including the person's name, address, telephone number, driver's license number, social security number, place of employment, maiden name of the person's mother, demand deposit account number, checking or savings account number, credit card or debit card number, personal identification number, passwords or any other numbers or information that can be used to access a person's financial resources.</p>	
New York	<p>190.77 "Personal identifying information"</p> <p>Means a person's name, address, telephone number, date of birth, driver's license number, social security number, place of employment, mother's maiden name, financial services account number or code, savings account number or credit card account number or code, debit card number or code, automated teller machine number or code, taxpayer identification number, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or personal identification number, or any other name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person.</p>	

State	Identity Theft	Security Breach
North Carolina	<p>§ 14-113.20. "Identifying information"</p> <p>Includes the following:</p> <ol style="list-style-type: none"> (1) Social security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6). (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage. 	
North Dakota	<p>12.1-23-11 "Personal identifying information"</p> <p>Means any of the following:</p> <ol style="list-style-type: none"> a. An individual's name; b. An individual's address; c. An individual's telephone number; d. The distinguishing operator's license number assigned to an individual by the department of transportation under section 39-06-14; e. An individual's social security number; f. An individual's employer or place of employment g. An identification number assigned to the individual by the individual's employer; h. The maiden name of the individual's mother; i. The identifying number of a depository account in a financial institution; or j. An individual's birth, death, or marriage certificate 	

State	Identity Theft	Security Breach
Ohio	<p>2913.49. "Personal identifying information"</p> <p>Includes, but is not limited to, the following: the name, address, telephone number, driver's license, driver's license number, commercial driver's license, commercial driver's license number, state identification card, state identification card number, social security card, social security number, birth certificate, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, money market account number, mutual fund account number, other financial account number, personal identification number, password, or credit card number of a living or dead individual.</p>	<p>1347.12A6(a). "Personal information"</p> <p>Means, notwithstanding section 1347.01 of the Revised Code, an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:</p> <ul style="list-style-type: none"> (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.
Oklahoma	<p>§21-1533.1. Personal Information</p> <p>name, address, social security number, date of birth, place of business or employment, debit, credit or account numbers, driver license number, or any other personal identifying information of another person</p>	<p>§74-3113.1. "Personal information"</p> <p>Means the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:</p> <ul style="list-style-type: none"> a. social security number, b. driver license number, or c. account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial account of an individual.
Oregon	<p>165.800 "Personal identification"</p> <p>Includes, but is not limited to, any written document or electronic data that does, or purports to, provide information concerning:</p> <ul style="list-style-type: none"> (A) A person's name, address or telephone number; (B) A person's driving privileges; (C) A person's Social Security number or tax identification number; (D) A person's citizenship status or alien identification number; (E) A person's employment status, employer or place of employment; (F) The identification number assigned to a person by a person's employer; (G) The maiden name of a person or a person's mother; (H) The identifying number of a person's depository account at a financial institution, as defined in ORS 706.008, or a credit card 	

State	Identity Theft	Security Breach
	<p>account;</p> <p>(I) A person's signature or a copy of a person's signature;</p> <p>(J) A person's electronic mail name, electronic mail signature, electronic mail address or electronic mail account;</p> <p>(K) A person's photograph;</p> <p>(L) A person's date of birth; and</p> <p>(M) A person's personal identification number</p>	
Pennsylvania	<p>18 Pa. Code 4120. "Identifying information."</p> <p>Any document, photographic, pictorial or computer image of another person, or any fact used to establish identify, including, but not limited to, a name, birth date, Social Security number, driver's license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number or, employee or payroll number or electronic signature.</p>	
Rhode Island	<p>§ 11-49.1-2. "Means of identification"</p> <p>Means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:</p> <p>(i) Name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;</p> <p>(ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;</p> <p>(iii) Unique electronic identification number, address, or routing code; or</p> <p>(iv) Telecommunication identifying information or access device as defined in 18 U.S.C. § 1029(e).</p>	<p>§ 11-49.2-5. "Personal information"</p> <p>Means 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:</p> <p>(1) Social security number;</p> <p>(2) Driver's license number or Rhode Island Identification Card number;</p> <p>(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.</p>
South Carolina	<p>Section 16-13-510. Identifying information</p> <p>Includes, but is not limited to:</p> <p>(1) social security numbers;</p> <p>(2) driver's license numbers;</p> <p>(3) checking account numbers;</p> <p>(4) savings account numbers;</p> <p>(5) credit card numbers;</p> <p>(6) debit card numbers;</p>	

State	Identity Theft	Security Breach
	<p>(7) personal identification numbers;</p> <p>(8) electronic identification numbers;</p> <p>(9) digital signatures;</p> <p>(10) other numbers or information which may be used to access a person's financial resources; or</p> <p>(11) identifying documentation that defines a person other than the person presenting the document. This includes, but is not limited to, passports, driver's licenses, birth certificates, immigration documents, and state-issued identification cards.</p>	
South Dakota	<p>22-40-9. Identifying information</p> <p>For the purposes of §§ 22-40-8 to 22-40-10, inclusive, identifying information includes:</p> <p>(1) Birth certificate or passport information;</p> <p>(2) Driver's license numbers;</p> <p>(3) Social security or other taxpayer identification numbers;</p> <p>(4) Checking account numbers;</p> <p>(5) Savings account numbers;</p> <p>(6) Credit card numbers;</p> <p>(7) Debit card numbers;</p> <p>(8) Personal identification numbers, passwords, or challenge questions;</p> <p>(9) User names or identifications;</p> <p>(10) Biometric data; or</p> <p>(11) Any other numbers, documents, or information which can be used to access another person's financial resources.</p>	
Tennessee	<p>39-14-150. "Personal identifying information"</p> <p>Means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including:</p> <p>(1) Name, social security number, date of birth, official state or government issued driver license or identification number, alien registration number, passport number, employer or taxpayer identification number;</p> <p>(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;</p> <p>(3) Unique electronic identification number, address, routing code or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data; or</p> <p>(4) Telecommunication identifying information or access device.</p>	

State	Identity Theft	Security Breach
Texas	<p>§ 48.002. "Personal identifying information"</p> <p>Means information that alone or in conjunction with other information identifies an individual, including an individual's:</p> <p>(A) name, social security number, date of birth, or government-issued identification number;</p> <p>(B) mother's maiden name;</p> <p>(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;</p> <p>(D) unique electronic identification number, address, or routing code; and</p> <p>(E) telecommunication access device.</p>	<p>§ 48.002. "Sensitive personal information":</p> <p>(A) means an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:</p> <p>(i) social security number;</p> <p>(ii) driver's license number or government-issued identification number; or</p> <p>(iii) account number or 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; and</p> <p>(B) does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.</p>
Utah	<p>76-6-1102 "Personal identifying information"</p> <p>May include:</p> <p>(a) name;</p> <p>(b) address;</p> <p>(c) telephone number;</p> <p>(d) driver's license number;</p> <p>(e) Social Security number;</p> <p>(f) place of employment;</p> <p>(g) employee identification numbers or other personal identification numbers;</p> <p>(h) mother's maiden name;</p> <p>(i) electronic identification numbers;</p> <p>(j) electronic signatures under Title 46, Chapter 4, Uniform Electronic Transactions Act; or</p> <p>(k) any other numbers or information that can be used to access a person's financial resources or medical information, except for numbers or information that can be prosecuted as financial transaction card offenses under Sections 76-6-506 through 76-6-506.4</p>	<p>13-44-102. "Personal information"</p> <p>Means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:</p> <p>(i) Social Security number;</p> <p>(ii) (A) financial account number, or credit or debit card number; and</p> <p>(B) any required security code, access code, or password that would permit access to the person's account; or</p> <p>(iii) driver license number or state identification card number.</p> <p>"Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.</p>

State	Identity Theft	Security Breach
Vermont	<p>§ 2030 "Personal identifying information"</p> <p>Includes name, address, birth date, Social Security number, motor vehicle personal identification number, telephone number, financial services account number, savings account number, checking account number, credit card number, debit card number, picture, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-mail address, computer system password, or mother's maiden name, or similar personal number, record, or information.</p>	<p>§ 2430. "Personal information"</p> <p>Means 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 or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:</p> <p>(i) Social Security number;</p> <p>(ii) Motor vehicle operator's license number or nondriver identification card number;</p> <p>(iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;</p> <p>(iv) Account passwords or personal identification numbers or other access codes for a financial account.</p>
Virginia	<p>§ 18.2-186.3. "identifying information"</p> <p>Shall include but not be limited to:</p> <p>(i) name;</p> <p>(ii) date of birth;</p> <p>(iii) social security number;</p> <p>(iv) driver's license number;</p> <p>(v) bank account numbers;</p> <p>(vi) credit or debit card numbers;</p> <p>(vii) personal identification numbers (PIN);</p> <p>(viii) electronic identification codes;</p> <p>(ix) automated or electronic signatures;</p> <p>(x) biometric data;</p> <p>(xi) fingerprints;</p> <p>(xii) passwords; or</p> <p>(xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services.</p>	

State	Identity Theft	Security Breach
Washington	<p>9.35.005. "Means of identification"</p> <p>Means information or an item that is not describing finances or credit but is personal to or identifiable with an individual or other person, including: A current or former name of the person, telephone number, an electronic address, or identifier of the individual or a member of his or her family, including the ancestor of the person; information relating to a change in name, address, telephone number, or electronic address or identifier of the individual or his or her family; a social security, driver's license, or tax identification number of the individual or a member of his or her family; and other information that could be used to identify the person, including unique biometric data.</p>	<p>42.56.590. "Personal information"</p> <p>Means 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:</p> <p>(a) Social security number;</p> <p>(b) Driver's license number or Washington identification card number; or</p> <p>(c) Account number or 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.</p> <p>For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>
West Virginia	<p>61-3-54. Personal Information</p> <p>name, birth date, social security number or other identifying information of another person</p>	
Wisconsin	<p>943.201. "Personal identifying information"</p> <p>Means any of the following information:</p> <ol style="list-style-type: none"> 1. An individual's name. 2. An individual's address. 3. An individual's telephone number. 4. The unique identifying driver number assigned to the individual by the department of transportation under s. 343.17 (3) (a) 4. 5. An individual's social security number. 6. An individual's employer or place of employment. 7. An identification number assigned to an individual by his or her employer. 8. The maiden name of an individual's mother. 9. The identifying number of a depository account, as defined in s. 815.18 (2) (e), of an individual. 10. An individual's taxpayer identification number. 11. An individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a). 12. Any of the following, if it can be used, alone or in conjunction with any access device, to obtain money, goods, services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds: <ol style="list-style-type: none"> a. An individual's code or account number. 	

State	Identity Theft	Security Breach
	<p>b. An individual's electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier.</p> <p>c. Any other means of account access.</p> <p>13. An individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</p> <p>14. Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.</p> <p>15. Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.</p>	
Wyoming	<p>6-3-901. Personal identifying information</p> <p>Means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, tribal identification card number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.</p>	

Appendix 2. Personal Information in Government Records

	Function	Description
1	Agriculture Industry	Airport release cards
2	Business Regulation and Consumer Affairs	Business registration, trade name/trademark/service mark registration, investigative files, financial institution license application forms, financial institution voluntary closure/merger, complaints, examination work papers, examination candidate roster and exam admission information, pleadings, exhibits, consumer complaints, banking records, tax information.
3	Economic Development	Loan applications, business plans/resume, credit rating, tax returns, personal financial information, licenses and contractor's wage reports
4	Elections	Notarial records, investigative reports, check copies (payment for fines and penalties), voter registration, candidate filing
5	Financial Administration	Unclaimed property program claims forms and data base
6	Health	Birth certificates, death certificates, marriage and divorce records, business entity documents, lease/rental agreements, criminal history and other background checks, licenses, ambulance report forms, ambulance fee waiver applications, medical records, authorization/consent forms, tax returns, financial information, vaccine administration records, adult foster home applications, substitute applications, adult protective services/child welfare services records, case management records, social security cards, laboratory reports
7	Housing	Rental assistance application, tenant certifications, tax returns, social security card, credit authorization form, credit reports, applications to purchase real property, application to purchase leased fee interest, tax clearance, leases, loan documents
8	Human Resources Management	Applications, identification cards, licenses, criminal history record clearance, police investigative reports, security clearance, emergency contact, certificate of medical examination, certification lists, timesheets, salary assignment, claim and payment records, Federal/State withholding, pay raise documents, payroll register, employee retirement system membership enrollment, employee designation of beneficiary, health fund, deferred compensation retirement plan, flexible spending accounts plan, grievance, training, personnel action, medical records, licenses, authorization/consents, vacation leave, injury reports
9	Human Services	Child care subsidy applications, bank statements, social services and welfare case records, applications for financial, food stamp and medical assistance, authorizations, reimbursement claims, adult abuse and neglect intake form, notification of foster parent placement, youth medical and dental records, youth mental health records

	Function	Description
10	Judicial	<p>Documents/records of active and disposed cases including civil actions (contracts, personal injury, property damage, motor vehicle, non-motor vehicle, condemnation, other civil actions and district court transfers), probate proceedings (probate intestate, testate, special administration, small estate, informal wills, other types), guardianship proceedings, trust proceedings and miscellaneous proceedings (land court, tax court, mechanic's and materialman's liens, other special proceedings), assumpsit, tort/other, summary possession, TRO's, decriminalized traffic cases, criminal actions (felonies, misdemeanors, petty misdemeanors, traffic criminal violations).</p> <p>Family Court legal records not generally available to the general public include divorce, paternity, adoption, guardianship, interstate custody and child support, juvenile law violation and status offense cases, child abuse and neglect cases, abuse of dependent adult, domestic abuse protective orders, criminal cases involving abuse of family or household members, and cases related to incapacitated persons.</p> <p>Personal information may be included in the legal pleadings relating to confidential divorce, adoption, child support, and guardianship cases and in supplemental financial, medical real property and other records. Such personal information may also be included in social records relating these parties.</p>
11	Labor	<p>Refugee date of entry, employer/claimant appeal records, wage complaints, child labor application forms, case files, discrimination complaint investigation records, workers' compensation case files, temporary disability insurance denial files, prepaid health care premium supplementation fund files, audit files, unemployment claims records, claimant payment/overpayment/collection, job training and employment applications, job training eligibility/enrollment records, employment and apprenticeship program records, on the job training contracts</p>
12	Land and Natural Resources Management	<p>Hunting license applications and licenses, freshwater fishing licenses, applications for mooring permits and wait lists, commercial operators permit, bank records identifying land ownership, genealogical information, conveyance documents</p>
13	Legal Compliance	<p>Tax records, credit reports and applications, employment records, loan application, teacher license applications, child support orders, notices, exhibits, criminal history records, sex offender registration, state identification records, workers' compensation, wage claims, work injury files, unemployment insurance, employee retirement, agricultural loans and/or leases, notary commission application, petitions for name change, petitions for involuntary records, criminal justice records, police reports, child support records, claims for wage loss and law enforcement databases.</p>
14	Procurement Management	<p>Procurement contract files, vendor tables, tax clearance documents, provider resumes, Pcard requests and transaction documents, Form 1099 Misc Statements</p>
15	Public Safety	<p>Inmate and pretrial supervision records, parole determination and supervision records, warrants, traffic reports, investigative reports, booking log, emergency incidents, controlled substance prescription records, crime victim compensation records</p>
16	Risk Management	<p>Insurance claim files</p>

	Function	Description
17	Tax	Business license applications, liquor, fuel and tobacco permit applications, personal checks and bank records, tax returns, extensions and estimated tax forms, taxpayer records and correspondence, tax assessments, billing notices,
18	Transportation	Disadvantaged business enterprise applications, individual tax return of business owners, investigation reports, security access lists, investigation reports, maritime security information, port security grants processing records, reallocation surveys, real property deeds, easements and other conveyance documents.

Appendix 3. Volume of Government Records Containing Personal Information

Ref	Department Agency	Record Volume	Annual Records Increase
10101	Department of Accounting and General Services	500,001 – 1,000,000	1% - 5%
10201	Department of Agriculture	100,001 – 500,000	1% - 5%
10301	Department of the Attorney General	1,000,001 or more	6% - 10%
10401	Department of Budget and Finance	500,001 – 1,000,000	1% - 5%
10501	Department of Business, Economic Development & Tourism	100,001 – 500,000	1% - 5%
10601	Department of Commerce and Consumer Affairs	1,000,001 or more	6% - 10%
10701	Department of Defense	100,001 – 500,000	26% - 50%
10801	Department of Education	500,000 - 1,000,000	6% - 10%
10901	Department of Hawaiian Home Lands	10,001 – 100,000	11% - 25%
11001	Department of Health	1,000,001 or more	26% - 50%
11101	Department of Human Resources Development	500,0001 -1,000,000	11% - 25%
11201	Department of Human Services	1,000,001 or more	1% - 5%
11301	Department of Labor and Industrial Relations	1,000,001 or more	1% - 5%
11401	Department of Land and Natural Resources	1,000,0001 or more	6% - 10%
11501	Department of Public Safety	1,000,001 or more	11% - 25%
11601	Department of Taxation	1,000,001 or more	6% - 10%
11701	Department of Transportation	500,001 – 1,000,000	1% - 5%
11705	Oahu Metropolitan Planning Organization	1 – 100	1% - 5%
11801	University of Hawaii	500,001 – 1,000,000	6% - 10%
11901	East-West Center	NR	NR
12001	The Judiciary	1,000,001 or more	11% - 25%
12101	Office of Hawaiian Affairs	101 – 1,000	1% - 5%
20101	City and County of Honolulu , Office of the Mayor	1 – 100	1% - 5%
20103	C&C Honolulu, Office of Managing Director	NR	
20201	C&C Honolulu, Office of the City Clerk	500,001 – 1,000,000	6% - 10%
20301	C&C Honolulu, Office of Council Services	101 – 1,000	6% - 10%

Ref	Department Agency	Record Volume	Annual Records Increase
20401	C&C Honolulu, Liquor Commission	NR	NR
20501	C&C Honolulu, Office of Economic Development	1 – 100	1% - 5%
20601	C&C Honolulu, Department of the Prosecuting Attorney	10,001 – 100,000	1% - 5%
20701	C&C Honolulu, Department of Budget & Fiscal Services	NR	NR
20801	C&C Honolulu, Customer Services Department	500,001 – 1,000,000	1% - 5%
20901	C&C Honolulu, Department of Enterprise Services	10,001 – 100,000	1% - 5%
21001	C&C Honolulu, Department of Design & Construction	101 – 1,000	1% - 5%
21101	C&C Honolulu, Department of the Corporation Counsel	10,001 – 100,000	1% - 5%
21201	C&C Honolulu, Department of Information Technology	1,000,001 or more	1% - 5%
21301	Honolulu Fire Department	1,001 – 10,000	6% - 10%
21401	C&C Honolulu, Department of Emergency Services	1,000,001 or more	6% - 10%
21501	C&C Honolulu, Department of Community Services	100,001 – 500,000	26% - 50%
21601	C&C Honolulu, Department of Planning & Permitting	1,001 – 10,000	1% - 5%
21701	C&C Honolulu, Department of the Medical Examiner	100,001 – 500,000	1% - 5%
21801	C&C Honolulu, Department of Parks & Recreation	500,001 – 1,000,000	11% - 25%
21901	C&C Honolulu, Department of Human Resources	10,001 – 100,000	6% - 10%
22001	Honolulu Police Department	1,000,001 or more	1% - 5%
22101	C&C Honolulu, Department of Facility Maintenance	1,001 – 10,000	1% - 5%
22201	C&C Honolulu, Department of Transportation Services	101 – 1,000	1% - 5%
22301	C&C Honolulu, Department of Environmental Services	1,001 – 10,000	1% - 5%
22401	C&C Honolulu, Board of Water Supply	100,001 – 500,000	1% - 5%

Ref	Department Agency	Record Volume	Annual Records Increase
22501	Oahu Civil Defense Agency	NR	NR
22601	Honolulu Ethics Commission	1 – 100	0%
30101	County of Hawaii, Office of the Mayor	1 – 100	11% - 25%
30201	County of Hawaii, County Clerk	100,001 – 500,000	1% - 5%
30301	County of Hawaii, Prosecuting Attorney's Office	10,001 – 100,000	1% - 5%
30401	County of Hawaii, Civil Defense Agency	1,001 – 10,000	1% - 5%
30501	County of Hawaii, Department of Civil Service	NR	NR
30601	County of Hawaii, Office of the Corporation Counsel	10,001 – 100,000	1% - 5%
30701	County of Hawaii, Department of Data Systems	1,001 – 10,000	1% - 5%
30801	County of Hawaii, Department of Environmental Management	NR	NR
30901	County of Hawaii, Department of Finance	100,001 – 500,000	6% - 10%
31001	Hawaii Fire Department	10,001 – 100,000	11% - 25%
31006	County of Hawaii, Office of Housing & Community Development	NR	NR
31101	County of Hawaii, Department of Human Resources	100,001 – 500,000	26% - 50%
31201	County of Hawaii, Department of Liquor Control	1,001 – 10,000	1% - 5%
31301	County of Hawaii, Mass Transit Agency	101 – 1,000	1% - 5%
31401	County of Hawaii, Department of Parks & Recreation	10,001 – 100,000	6% - 10%
31501	County of Hawaii, Planning Department	NR	NR
31601	Hawaii Police Department	1,000,001 or more	11% - 25%
31701	County of Hawaii, Department of Public Works	1,001 – 10,000	0%
31801	County of Hawaii, Department of Research & Development	101 – 1,000	6% - 10%
40101	County of Hawaii, Department of Water Supply	10,001 – 100,000	1% - 5%
40101	County of Kauai, Office of the Mayor	1 – 100	0%
40701	County of Kauai, Office of the Prosecuting Attorney	NR	NR

Ref	Department Agency	Record Volume	Annual Records Increase
40801	County of Kauai, Department of Liquor Control	1,001 – 10,000	1% - 5%
40901	Kauai Fire Department	10,001 – 100,000	1% - 5%
41001	Office of the County Attorney-County of Kauai	101 – 1,000	6% - 10%
41101	Department of Finance-County of Kauai	10,001 – 100,000	NR
41201	Department of Personnel Services-County of Kauai	1,001 – 10,000	1% - 5%
41301	Department of Planning-County of Kauai	1 – 100	1% - 5%
41401	Kauai Police Department	100,001 – 500,000	6% - 10%
41501	Department of Public Works-County of Kauai	100,001 – 500,000	6% - 10%
41601	Department of Transportation-County of Kauai	NR	NR
41701	County of Kauai, Department of Water	101 – 1,000	1% - 5%
41801	Civil Defense Agency-County of Kauai	1 – 100	0%
41901	County of Kauai, Office of Economic Development	101 – 1,000	1% - 5%
42001	Office of Community Assistance-County of Kauai	10,001 – 100,000	1% - 5%
50101	County of Maui, Office of the Mayor	1 – 100	0%
50201	County of Maui, Office of the Managing Director	NR	NR
50301	Office of the Prosecuting Attorney-County of Maui	10,001 – 100,000	11% - 25%
50401	Department of the Corporation Counsel-County of Maui	101 – 1,000	1% - 5%
50501	Department of Finance-County of Maui	1,000,001 or more	6% - 10%
50601	Department of Fire Control-County of Maui	101 – 1,000	1% - 5%
50701	Dept. of Housing & Human Concerns-County of Maui	10,001 – 100,000	6% - 10%
50801	Department of Liquor Control-County of Maui	NR	NR
50901	Department of Parks & Recreation-County of Maui	1,001 – 10,000	11% - 25%
51001	Department of Personnel Services-County of Maui	500,001 – 1,000,000	1% - 5%
51101	Department of Planning-County of Maui	NR	NR

Ref	Department Agency	Record Volume	Annual Records Increase
51201	Department of Police-County of Maui	1,000,001 or more	1% - 5%
51301	Dept. of Public Works & Env. Mgt.-County of Maui	10,001 – 100,000	11% 25%
51401	Department of Water Supply-County of Maui	1,001 – 10,000	1% - 5%
51501	Civil Defense Agency-County of Maui	NR	NR
51601	Department of Transportation-County of Maui	1 – 100	1% - 5%

NR = No Response

Appendix 4. Best Practices in Other State Jurisdictions

State		Description	Comments
Arizona			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§13-2008 – 13-2010 Taking Identity of Another Person
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	Sec. 44-7501
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Arizona Crime Victims Website (http://www.azdps.gov/azvictims/identity/default.asp) Dept of Public Safety (http://www.azdps.gov/azvictims/identity/default.asp); Dept of Attorney General (http://www.azag.gov/cybercrime/ID_Theft.html)
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Identity theft brochure. http://www.douglasaz.gov/StateInformation/IDTheftBrochure.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Connecticut			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Sec. 53a-129a. Identity theft defined
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	Sec. 36a-701b
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	The Governor's Identity Theft Information Team formed in 2006
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Delaware			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Title 11 of the Delaware Code Relating to Identity Theft, Section 828
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 12B-102. Disclosure of breach of security of computerized personal information by an individual or a commercial entity.
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	§ 12B-102. Disclosure of breach of security of computerized personal information by an individual or a commercial entity.
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	§ 9018C. Development and implementation of agency privacy policies.
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	§854A. Identity theft passport; application; issuance Delaware Administrative Code Title 6 Attorney's General Office, Identity Theft Passport

State		Description	Comments
District of Columbia			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§22-3227.02. Identity Theft
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Metropolitan Police, http://mpdc.dc.gov/mpdc/cwp/view,a,1237,Q,543161.asp Office of the Attorney General, http://oag.dc.gov/occ/cwp/view,a,1223,q,635085.asp
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Florida			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§817.568 Criminal use of personal identification information
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	817.5681 Breach of security concerning confidential personal information in third-party possession; administrative penalties.--
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Agriculture and Consumer Services, http://www.800helpfla.com/identity.html Office of the Attorney General, http://www.myfloridalegal.com/identitytheft
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Georgia			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§ 16-9-121. Elements of offense
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 10-1-912. Notification required upon breach of security regarding personal information
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	Office of Consumer Affairs, http://consumer.georgia.gov/00/article/0,2086,5426814_39039081_39480072,00.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	§ 16-9-123. Investigations

State		Description	Comments
Hawaii			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§708-839.8 Identity theft in the third degree
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§487N-2 Notice of security breach
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	§487N-2 Notice of security breach
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of the Attorney General, http://www.hawaii.gov/ag/hitec/main/Identity%20Theft/ Department of Commerce and Consumer Affairs, http://www.hawaii.gov/dcca/quicklinks/id_theft_info/
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Idaho			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Idaho Code 18-3126
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	28-51-105. Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	28-51-105. Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	28-51-106. Procedures deemed in compliance with security breach requirements
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	http://www2.state.id.us/ag/consumer/tips/IdentityTheft.pdf http://idaho.gov/cyber/identity_theft.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	http://isp.state.id.us/ID%20Theft.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Illinois			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	(720 ILCS 5/16G-20) Sec. 16G-20. Aggravated identity theft
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	(815 ILCS 530/10) Sec. 10. Notice of Breach
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	(815 ILCS 530/12) Sec. 12. Notice of breach; State agency
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Attorney General, http://www.illinoisattorneygeneral.gov/consumers/idtheft.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	ID Theft Hotline, http://www.illinoisattorneygeneral.gov/consumers/brochure_idtheft.pdf Attorney General ID Theft Resource Guide, http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Indiana			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	IC 35-43-5-3.5 Identity deception
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	IC 24-4.9-3 Chapter 3. Disclosure and Notification Requirements
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Insurance, http://www.in.gov/doi/consumer_services/identity_theft.html Department of Financial Institutions, http://www.in.gov/dfi/education/IdThieve.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	IC 4-1-6-2 Personal information system
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Department of Financial Institutions, http://www.in.gov/dfi/education/identity_crisis.htm
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Iowa			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	714.16B Identity Theft
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Transportation, http://www.dot.state.ia.us/mvd/omve/theft.htm Attorney General, http://www.iowaattorneygeneral.org/consumer/brochures/avoid_identitytheft.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	61-2.8(17A,22) Notice to suppliers of information
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Attorney General Consumer Protection Division, http://www.state.ia.us/government/ag/consumer/brochures/Identity_Theft_GUIDE.pdf
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	715A.9A Identity Theft Passport

State		Description	Comments
Kansas			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	21-4018. Identity theft; identity fraud
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Bureau of Investigation, http://www.kansas.gov/kbi/PDF/brochures/Identity%20Theft.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Kentucky			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	514.160 Theft of Identity
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	Financial Integrity Enforcement Division, http://www.lrc.ky.gov/krs/015-00/113.pdf
	<input checked="" type="checkbox"/>	6. State Website	Office of Attorney General, http://ag.ky.gov/consumer/identity/
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Office of Attorney General, http://ag.ky.gov/NR/rdonlyres/03BEBF96-F293-4ED6-97D6-698216AA1CFD/0/idtheft_kit.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Louisiana			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	RS 14:67.16
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	RS 51:3074
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	RS 51:3074
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	Department of Justice, http://ag.louisiana.gov/publications/identitytheft.htm
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Maine			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Title 17-A: Maine Criminal Code, Part 2: Substantive Offenses, Chapter 37: Fraud, §905-A. Misuse of identification
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Bureau of Financial Institutions, http://www.maine.gov/pfr/financialinstitutions/consumer/credit_report.htm Office of the Maine Attorney General, http://www.maine.gov/ag/index.php?r=protection&s=identitytheft&t= Department of Professional and Financial Regulation, http://www.maine.gov/pfr/consumercredit/documents/identity_theft.htm Secretary of State, http://www.maine.gov/sos/IDFraud.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	Title 1: General Provisions, Chapter 14-A: Notice of Information Practices (HEADING: PL 2001, c. 321, Pt. B, §1 (new)), §542. Notice of information practices
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Maryland			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	8-301 Identity Fraud
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	Electronic Transaction Education, Advocacy, and Mediation Unit in the Office of the Attorney General
	<input checked="" type="checkbox"/>	6. State Website	Commissioner of Financial Regulation, http://www.dllr.state.md.us/finance/identitytheft.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	10-624 Personal Records
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	8-305 Identity Theft Passport

State		Description	Comments
Massachusetts			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Chapter 266: Section 37E
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Executive Office of Public Safety, http://www.mass.gov/?pageID=eopssubtopic&L=3&L0=Home&L1=Crime+Prevention+%26+Personal+Safety&L2=Identity+Theft&sid=Eeops Office of Consumer Affairs and Business Regulation, http://www.mass.gov/?pageID=ocasubtopic&L=4&L0=Home&L1=Consumer&L2=National+Consumer+Protection+Week+Tips&L3=Identity+Theft&sid=Eoca
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Michigan			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Identity Theft Protection Act, 445.65 Prohibited acts; violations; defense in civil action or criminal prosecution; burden of proof
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	445.72. Notice of security breach; requirements. Allows exceptions in instances that a determination can be made that no harm will result from breach
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	445.72. Notice of security breach; requirements.
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	Michigan State Police Identity Theft Unit, http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html
	<input checked="" type="checkbox"/>	6. State Website	http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Identity Theft Investigation Training, http://www.michigan.gov/msp/0,1607,7-123-1586_1710-146826--,00.html
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Minnesota			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	609.527 Identity Theft
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	13.055 State Agencies, Disclosure of Breach in Security
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	Financial Crimes Oversight Council and Task Force, http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&year=2006&section=299A.681&keyword_type=exact&keyword=identity+theft
	<input checked="" type="checkbox"/>	6. State Website	Department of Commerce, http://www.state.mn.us/portal/mn/jsp/content.do?id=-536881350&subchannel=-536882973&contentid=536885792&contenttype=EDITORIAL&programid=536899774&sp2=y&agency=Commerce
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Office of the Attorney General, http://www.ago.state.ms.us/divisions/consumer/ Office of the Attorney General, ID Theft Guidebook, http://www.ago.state.ms.us/divisions/consumer/idtheftbook.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Missouri			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	570.223. 1. Identity theft--penalty--restitution--other civil remedies available--exempted activities.
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Office of the Attorney General, Consumer Protection Division, http://www.ago.state.ms.us/divisions/consumer/idtheftbook.pdf
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	Privacy of Computer-accessible, Confidential Personal Information, http://www.sos.mo.gov/adrules/csr/current/1csr/1c10-2.pdf
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Discovered	<i>Missouri Revised Statutes</i> , Chapter 59 , County Recorders of Deeds , Section 59.331
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Missouri State Highway Patrol, Brochure, http://www.mshp.dps.mo.gov/MSPWeb/Publications/Brochures/SHP-188.pdf Office of the Attorney General, ID Theft Hotline http://www.ago.mo.gov/newsreleases/2005/072805.htm
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Montana			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	45-6-332. Theft of identity
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Justice, http://doj.mt.gov/consumer/consumer/identitytheft.asp
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	46-24-220. Identity theft passport -- application -- issuance

State		Description	Comments
Nebraska			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	Section 28-608, Criminal impersonation; penalty; restitution
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	Section 87-803 Breach of security; investigation; notice to resident.
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	Section 87-803 Breach of security; investigation; notice to resident.
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	Section 87-804 Compliance with notice requirements; manner
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Nebraska CyberSecurity Center, http://its.ne.gov/cybersecurity/idtheft/
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Nebraska Department of Justice, Understanding Identity Theft, http://www.ago.state.ne.us/content/Id_Theft_p1.pdf Nebraska Department of Motor Vehicles, Identity Theft Complaint Packet, http://www.dmv.state.ne.us/dvr/pdf/theftpacket.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Nevada			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	NRS 205.463 Obtaining and using personal identifying information of another person to harm person or for unlawful purpose; penalties. NRS 205.464 Obtaining, using, possessing or selling personal identifying information for unlawful purpose by public officer or public employee; penalties.
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Nevada Attorney General, http://ag.state.nv.us/menu/action_btn/programs/cyber_crime/victim.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	NRS 239B.030 Confidentiality of social security numbers, http://search.leg.state.nv.us/isysquery/irl3b62/5/doc
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Nevada Attorney General, Bureau of Consumer Protection, http://ag.state.nv.us/menu/top/newsroom/press_release/2007/NCPW2007IDTheft-CreditReports.pdf
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	Nevada Attorney General, Identity Theft Passport Program, NRS 205.4651 Identity Theft Passport, http://ag.state.nv.us/menu/passport/introduction.htm

State		Description	Comments
New Hampshire			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	638:26 Identity Fraud
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	7-A:2 File With Secretary of State
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
New Jersey			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	2C:21-17.2 Use of personal identifying information of another, certain; second degree crime
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	C.56:8-163 Disclosure of breach of security to customers
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	C.56:8-163 Disclosure of breach of security to customers
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Office of the Attorney General, http://www.state.nj.us/lps/ca/idtheft.htm Department of Banking and Insurance, http://www.state.nj.us/dobi/identitytheft.htm New Jersey State Police, http://www.state.nj.us/njsp/tech/identity.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	C.56:8-164 Prohibited actions relative to display of social security numbers
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Office of Attorney General, Division of Consumer Affairs, Brochure, http://www.state.nj.us/lps/ca/brief/idtheft.pdf Guide to Business, http://www.state.nj.us/lps/ca/brief/idtheftbus.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
New Mexico			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	30-16-24.1 Theft of Identity
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Attorney General Office, http://www.ago.state.nm.us/know/idtheft/idtheft.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Attorney General Office, http://www.ago.state.nm.us/know/idtheft/identity_theft.pdf Regulation & Licensing Department, Foiling Identity Theft Brochure, http://www.rld.state.nm.us/Securities/PDFs/IDtheftBrochure.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
New York			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	NY CLS Penal 190.77-190.84
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	New York State Police, http://www.troopers.state.ny.us/Publications/Crime_Prevention/Text_Only/IdentityTheft.cfm New York State Banking Department, http://www.banking.state.ny.us/brid.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	New York State Police, Brochure, http://www.troopers.state.ny.us/Publications/Crime_Prevention/idtheft.pdf New York State Consumer Board, A Consumer Guide to Preventing and Responding to Identity Theft, http://www.consumer.state.ny.us/pdf/id_theft_online_version.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
North Carolina			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§ 14-113.20. Financial Identity Fraud
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 75-65. Protection from security breaches
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Transportation, Division of Motor Vehicles, http://www.ncdot.org/dmv/other_services/licenset theft/identityTheft.html
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	§ 132-1.10. Social security numbers and other personal identifying information
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
North Dakota			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	N.D.C.C. 12.1-23-11
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Insurance Department, http://www.nd.gov/ndins/consumer/details.asp?ID=249 Office of Attorney General, http://www.ag.nd.gov/CPAT/IDTheft/IDTheft.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Office of Attorney General, Brochure, http://www.ag.nd.gov/Brochures/FactSheet/IdentityTheft.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Ohio			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	2913.49 Identity fraud
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	1347.12 Agency disclosure of security breach of computerized personal information data
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Attorney General, http://www.ag.state.oh.us/spotlight/idtheft.asp Department of Public Safety, http://bmv.ohio.gov/driver_license/id_fraud.htm
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	1347.05 Duties of state and local agencies maintaining personal information systems.
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	317.082 Social security number not to be included in document filed for recording.
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Attorney General, Victim Assist Kit, http://www.ag.state.oh.us/victim/idtheft/victim_assistance_kit.pdf
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	ID Theft Verification Passport, http://www.ag.state.oh.us/victim/idtheft/index.asp

State		Description	Comments
Oklahoma			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§21-1533.1. Identity theft - Penalties - Civil action
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	No requirement for private sector entities
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	§74-3113.1. Disclosure of breach of security of computerized personal information
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	§22-19b. Oklahoma Identity Theft Passport Program

State		Description	Comments
Oregon			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	165.800 Identity theft
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Department of Motor Vehicle, http://www.oregon.gov/ODOT/DMV/driverid/idtheft.shtml Department of Justice, http://www.doj.state.or.us/finfraud/idtheft.shtml
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	802.177 Prohibition on release of personal information from motor vehicle records
	<input type="checkbox"/>	11. Educational/Outreach Programs	Department of Justice, Information Fact Sheet, http://www.doj.state.or.us/finfraud/facta.shtml
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Pennsylvania			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	18 Pa. Code 4120
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	Act 94 of 2005
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	Identity Theft Action Plan, http://www.identitytheftactionplan.com/
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	Department of Public Welfare, § 41.15. Copies of documents.
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Pennsylvania State Police, Brochure, http://www.psp.state.pa.us/psp/lib/psp/PSP_Identity_Theft.pdf Department of Banking, Brochure, http://www.banking.state.pa.us/banking/lib/banking/financial_institutions/pamphletsbrochures/identity-theft-brochure-web.pdf Attorney General, Bureau of Consumer Protection, Brochure, http://www.attorneygeneral.gov/uploadedFiles/Consumers/identity_theft.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Rhode Island			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	11-49.1-1 to 11-49.1-5
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 11-49.2-3 Notification of breach
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	§ 11-49.2-3 Notification of breach
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	§ 11-49.2-7 Agencies with security breach procedures
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
South Carolina			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	Section 30-2-40
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Identity theft forums. http://www.sccoconsumer.gov/press_releases/2006/identity_theft-forum.pdf http://www.sccoconsumer.gov/publications/flyers/id_theft.pdf
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	Section 37-20-160

State		Description	Comments
South Dakota			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	22-40-8
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Tennessee			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	39-14-150
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Department of Safety. http://tennessee.gov/safety/cididtheft.htm Office of the Attorney General. http://www.attorneygeneral.state.tn.us/cpro/idtheft.htm http://www.attorneygeneral.state.tn.us/press/2005/story/PR2.pdf
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Texas			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§ 48.101
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 48.103
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected/Displayed/Disclosed	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Department of Public Safety. http://www.txdps.state.tx.us/administration/driver_licensing_control/idtheft/idtheft2.htm Texas Attorney General. http://www.oag.state.tx.us/consumer/idtheft.shtml
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	§ 48.202

State		Description	Comments
Utah			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	76-6-1102. Identity fraud crime
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	13-44-202. Applies only to computerized data.
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	13-45-301 (Effective 09/01/08). Protection of personal information. The state, or a branch, agency, or political subdivision of the state, may not employ or contract for the employment of an inmate in any Department of Corrections facility or county jail in any capacity that would allow any inmate access to any other person's personal information.
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	13-44-202. Personal information -- Disclosure of system security breach
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	67-5-22. Identity theft reporting information system

State		Description	Comments
Vermont			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§ 2030. Identity theft
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	§ 2435. Notice of security breaches
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	Exemption repealed as of June 30, 2008
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Virginia			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	§ 18.2-186.3
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	§ 2.2-3803
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected	§ 2.2-3803
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Virginia Attorney General. http://www.oag.state.va.us/FAQs/FAQ_IDTheft.html http://www.oag.state.va.us/FAQs/IDTheftBook02.pdf
	<input checked="" type="checkbox"/>	12. Identity Theft Registry	§ 18.2-186.5.

State		Description	Comments
Washington			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	9.35.020
	<input checked="" type="checkbox"/>	2. Notification Requirement for Personal Information Breach	19.255.010
	<input checked="" type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	42.56.590
	<input checked="" type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	42.56.590
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input checked="" type="checkbox"/>	6. State Website	http://www.atg.wa.gov/ConsumerIssues/ID-Privacy.aspx
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input checked="" type="checkbox"/>	9. State Agency Information Use Notice	74.18.127
	<input type="checkbox"/>	10. Restricts Personal Information Collected	
	<input checked="" type="checkbox"/>	11. Educational/Outreach Programs	Attorney General. http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/IdentityTheft.aspx
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
West Virginia			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	61-3-54
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	5. Dedicated State Agency	
	<input type="checkbox"/>	6. State Website	
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input type="checkbox"/>	10. Restricts Personal Information Collected	
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Wisconsin			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	943.201(individual) and 943.201(entity)
	<input type="checkbox"/>	2. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	3. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	4. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input checked="" type="checkbox"/>	5. Dedicated State Agency	Office of Privacy Protection
	<input checked="" type="checkbox"/>	6. State Website	http://privacy.wi.gov/
	<input type="checkbox"/>	7. Publishes Best Practices Guidance	
	<input type="checkbox"/>	8. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	9. State Agency Information Use Notice	
	<input checked="" type="checkbox"/>	10. Restricts Personal Information Collected	19.62
	<input type="checkbox"/>	11. Educational/Outreach Programs	
	<input type="checkbox"/>	12. Identity Theft Registry	

State		Description	Comments
Wyoming			
	<input checked="" type="checkbox"/>	1. Identity Theft Specific Misdemeanor/Felony Sanction	6-3-901
	<input type="checkbox"/>	13. Notification Requirement for Personal Information Breach	
	<input type="checkbox"/>	14. Requirements for Personal Information Protection Includes Government Agencies	
	<input type="checkbox"/>	15. Offers Preemption if Governed by State/federal Statute that Provides Stronger Protection and More Thorough Disclosure Notification Requirements	
	<input type="checkbox"/>	16. Dedicated State Agency	
	<input type="checkbox"/>	17. State Website	
	<input type="checkbox"/>	18. Publishes Best Practices Guidance	
	<input type="checkbox"/>	19. Publishes Guidance on Information Breach Notification	
	<input type="checkbox"/>	20. State Agency Information Use Notice	
	<input type="checkbox"/>	21. Restricts Personal Information Collected	
	<input type="checkbox"/>	22. Educational/Outreach Programs	
	<input type="checkbox"/>	23. Identity Theft Registry	

Appendix 5. Brochure for Businesses

This page intentionally left blank

PROTECT YOUR BUSINESS

Guard Your Customers' Information

Identity thieves are targeting businesses from large companies to small stores seeking to steal customers' and employees' personal information. Here are some tips to help your business keep this information out of the hands of identity thieves.

COLLECTION OF PERSONAL INFORMATION

Avoid asking your customers for private information, unless no other option is available.

Stop using Social Security Numbers or driver's license numbers as account numbers.

Don't collect SSNs on job applications until selecting the applicant. Once you've selected a prospective new employee, consider conducting criminal and civil background checks, particularly if the employee will have access to sensitive information.

Pick passwords and usernames that don't include personal information.

Avoid asking customers to provide you with necessary personal information in front of other customers or where the information could be seen or overheard.

Turn computer screens away from public view.

PROTECT PERSONAL INFORMATION

Limit customers and vendors to designated public areas.

Limit access to documents and files that contain personal identifying information to key managers who need to see it.

When an employee leaves, immediately remove their access to computer networks and confidential files.

Verify third party requests for personal information by contacting the requesting agency and taking reasonable steps to make sure they have a legitimate purpose for getting the information.

Implement security procedures for safeguarding documents that contain personal identifying information.

Keep documents containing personal information in locked cabinets. At a minimum, ensure that all vital records and offices are locked during non-business hours.

Regularly brief employees and management about security policies, security threats, corrective measures and incident reporting procedures.

PROTECT COMPUTERS

Institute a laptop security policy.

Limit access to computers by using employee passwords.

Put additional security measures in place, such as firewalls, anti-virus software, spyware protection software, and encryption software.

Use data protection software that records network activity and regularly check logging data and audit trails for unusual or suspicious activity.

Avoid file sharing or access to files containing personal identifying information via a network or the Internet, unless it is absolutely necessary.

PROTECT CORRESPONDENCE

Keep incoming mail in a locked mailbox.

Don't mail, e-mail, or fax bills or other correspondence to customers that include personal identifying information.

Include only part of the employee or customer's SSN if it is necessary to include it at all.

DISPOSE OF PERSONAL INFORMATION

Shred or destroy documents and records containing personal identifying information when you dispose of them. At a minimum, employees should destroy old documents containing personal information using a cross-cut paper shredder.

Make old computers' hard-drives unreadable. After you back up your data and transfer the files elsewhere, you should sanitize by disk shredding, magnetically cleaning the disk, or using software to wipe the disk clean. Make sure there isn't additional hardware related to the company's local area network.

Destroy old computer disks and backup tapes.

Hawaii's New Identity Theft Laws

Under Hawaii's new identity theft laws, businesses must notify customers if they are at risk for identity theft due to a security breach. Under the Act, businesses must protect their customers by:

➤ Shredding or destroying documents they dispose of that include customers' personal information.

➤ Notifying their customers promptly if a security breach may have compromised their personal information and placed them at risk of identity theft.

➤ Notifying the Office of Consumer Protection of the breach. Failure to do so may result in penalties of up to \$2500 per violation.

APPENDIX 6. Summary of State and County Agencies Presentations to the Hawai'i ID Theft Task Force

In addition to the agencies in the table below, the Task Force heard presentations from the following agencies and organizations: State Judiciary; Department of Accounting and General Services, Information and Communications Services Division (ICSD); the Attorney General's Office; Symantec, Inc.; Hawaiian Electric Industries; and the Consumer Data Industry Association.

Personal information is defined as: 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 data elements are not encrypted: a. social security number; b. driver's license number or Hawai'i identification card number; or c. account number, credit or debit card number, access code, or password that would permit access to an individual's financial account (including credit cards issued to employees for agency purchase purposes).

<i>Questions</i>	County of Maui, Department of Finance	County of Hawai'i, Legislative Auditor	City and County of Honolulu, Department of Information Technology
<i>1. Kinds of personal information collected and stored</i>	Personnel records, business records (procurement, tax, licensing, service applications, liquor control), taxpayer records (drivers license, vehicle registration, real property information tax records, applications for service, police records, housing and human services applications for aid and services, refuse collection, application for water service	54 types of records for employees and voter registration information	Personnel records, driver training (employees), vendor records, liquor license, workers comp, police personnel, police firearm system, police ID system, juvenile justice information, prosecuting attorney case tracking system, drivers licensing, voter registration, subpoena system, police special duty system.
<i>2. Number of records containing personal information</i>	DMV – over 1 million Real property tax – over 500,000 Accounts – over 1 million Procurement – over 100,000 Police – over 1 million Liquor control – less than 1,000 Prosecuting attorney – 100,000 Water dept. – over 50,000 Housing & Human concerns – over 25,000 Personnel – over 500,000 Public works – over 10,000	100,000-500,000 records	Millions of records.
<i>3. Is personal information made available to third parties?</i>	Available to law enforcement, judiciary, state agencies, and federal agencies	Yes, to government and non-government agencies.	Employee Retirement System, Employer-Union Trust Fund, deferred compensation, union dues
<i>4. What policies and practices related to internal and external access and security of the information?</i>	No countywide policies or guidelines; departments have internal operating guidelines; IT security policy applies countywide; departments practice redaction of records	Policies are being updated. Internet and email policies.	DHRD policies on disclosure, protection of paper records, breach notification, disposal, and training. Since Nov. 2004, SSNs have not been used as employee ID numbers. Internet policy deals with network security.
<i>5. Is there one overall manager responsible for access and security within the agency or is responsibility dispersed?</i>	IT security countywide is under one dept.; departments responsible for records on systems not on county platforms	County Clerk, County Clerk's designee, Departmental Personnel Clerk, Information Security Officer	Different agencies are responsible for electronic and paper records

<i>Questions</i>	County of Maui, Department of Finance	County of Hawai'i, Legislative Auditor	City and County of Honolulu, Department of Information Technology
6. <i>Has there been any unauthorized access to personal information over the past several years?</i>	None reported	No known unauthorized access.	
7. <i>What training on confidentiality and handling of personal information is provided to staff?</i>	No countywide training program; some departments provide individual training	Individualized training by departmental personnel clerk. Departmental, ethics, and UIPA workshops. Mandatory information security training program being developed.	
8. <i>What is the agency's most critical need to assure security of personal information?</i>	Update record retention policy, more resources dedicated to IT security; more funding for security and consultants; more staff and resources	Update formal policies and procedures, ensure compliance with statutory requirements, formal ongoing mandatory staff training	
9. <i>What steps has the agency taken to comply with HRS Ch. 487J, 487N, and 487R?</i>	Departments are currently assessing; payroll system being modified to prevent display of SSN, tax records redacted before distribution, correspondence redacted for SSN	Information security and privacy plan to comply with the requirements of Ch. 487J and 487R have been drafted and should be finalized in the next six months.	
10. <i>Are there any physical or electronic based solutions in place to protect personal information?</i>	Locked areas, locked offsite storage, guidelines exist for utilizing stored information; IT security limits access on the county system	Office keys issued and acknowledged, "locked" computers, locks for desks and filing cabinets. Internet and email policy, computer access, levels of approved access, logins, firewalls, password policy.	City Human Resource Management System files to external agencies encrypted with PGP; access to mainframe production files controlled by Top Secret and the application
11. <i>Are there plans for any physical or electronic based solutions to protect personal information?</i>	Upgrades to HR system; performed a security assessment in late 2006 with follow up assessments and annual reviews; new IT system will restrict personal information available	Plans for education and training, file encryption, safeguarding personal information on removable storage, hard drive encryption on all laptops, biometric security, and increased network security.	

<i>Questions</i>	County of Maui, Department of Finance	County of Hawai'i, Legislative Auditor	City and County of Honolulu, Department of Information Technology
<i>12. Are the systems that contain personal information in one site or dispersed?</i>	Countywide IT systems are maintained on a centralized server system; hard copy records at departments or stored offsite	At different locations.	
<i>13. How does the agency dispose of physical and electronic records containing personal information?</i>	Departmental shredders and contractors; electronic records periodically archived	County currently reviewing and revising its record retention and destruction policies.	

Questions	Department of Education	Department of Human Services	Department of Health
<i>1. Kinds of personal information collected and stored</i>	Employee and student records. Student ID, not SSN, is used to identify students.	Client information including names, SSN, and bank account numbers	SSN for both personnel and customers; half of the programs use SSN; State P-card; Driver's license numbers
<i>2. Number of records containing personal information</i>	The electronic systems capacity for active and inactive records is: payroll – 1 million; personnel – 100,000; student information system – 300,000.	Serves 250,000 annually and over 2,800 employee records.	Estimate between 4.8 million and 7.7 million
<i>3. Is personal information made available to third parties?</i>	Yes, for background checks, teacher certification, payroll purposes.	When required by federal or state law, authorized by the individual.	To Social Security Administration, Medicare / Medicaid, Hansen's disease, EMS
<i>4. What policies and practices related to internal and external access and security of the information?</i>	DOE follows federal law (FERPA, HIPAA, IDEA), state law (HRS Ch. 34), and Board policy (4610 student information and confidential records.	Internal access, if permitted by policy, requires business need External access, if permitted by law, requires written request, review/redact information	There are no overall policies currently; HIPAA policies will be applied to the entire department by the end of the year and the HIPAA office will be responsible for policies; Employees sign an IT policy
<i>5. Is there one overall manager responsible for access and security within the agency or is responsibility dispersed?</i>	Decentralized security, fragmented in many departments and applications.	Deputy director is responsible for overall policy compliance; DHS Security incident response team and/or HIPAA compliance are responsible for investigations, audits, and enforcement Office of information technology is responsible for management of network access, systems security, and monitoring of network.	Dispersed
<i>6. Has there been any unauthorized access to personal information over the past several years?</i>	At least 2 incidents. In December 2005, 6 PCs were stolen from the Payroll Department. In February 2007, personal checks from 18 schools were taken in an armored car robbery.	None.	There were 3 breaches in 2006: Child mental health – mail sent to wrong provider; EMS – an employee took 576 report forms home; WIC – an employee had access to client SSNs
<i>7. What training on confidentiality and handling of personal information is provided to staff?</i>	Payroll and Accounting offices have written policy regarding nondisclosure of employee SSN, and FERPA is referenced as a guide for confidentiality of student records. There is an Internet Access Policy but no training.	Department wide DHS security policy training HIPAA privacy policy training Periodic security reminders.	Each program is responsible for training

Questions	Department of Education	Department of Human Services	Department of Health
8. <i>What is the agency's most critical need to assure security of personal information?</i>	Chief security office to mandate and monitor security; training and awareness, centralized security, accountability and monitoring, standardized disposal and destruction.	Funding /resources to implement security technologies, implement hardware and software, and audit and monitor compliance.	Money – the information system is fragmented, varies by program, uses custom programs; Require \$1 million but the current budget is \$180,000.
9. <i>What steps has the agency taken to comply with HRS Ch. 487J, 487N, and 487R?</i>	Have identified forms and reports that contain personal information, surveyed schools and offices on the volume of records, formed a taskforce to implement an action plan.	Reviewing current DHS practices; new policies regarding ID theft, breach notice, security policy training.	Policies on notification, destruction, SSN protection take effect in March 2007; security awareness training is planned for all employees beginning May, 2007
10. <i>Are there any physical or electronic based solutions in place to protect personal information?</i>	WAN network firewall and intrusion prevention centrally controlled, application level access security by roles, and inconsistent implementation of password security, encryption practices, destruction and transfer of electronic information, knowledge management.	Physical security policy on facility access controls, workstation usage and security, device and media controls Technical safeguards – role based access control, audit controls, authentication, and transmission security.	Mitigation – inventory, determine if necessary, destroy unnecessary records
11. <i>Are there plans for any physical or electronic based solutions to protect personal information?</i>	SSN protection through use of employee identification number, removing SSN from forms and reports, training. FERPA – revise admin rules, create standard practice document, educate parents and students Breach notification – create standard practice document, standard input form, educate DOE. Destruction and transfer of information – determine life cycle of data, create standard practice, and identify needs for contracted disposal. Chief security office.	Periodic risk assessment and remediation, audits, including intrusion testing, facility upgrades, plans for biometric and multi-factor authentication, and plans to scrub hard drives that are disposed.	
12. <i>Are the systems that contain personal information in one site or dispersed?</i>	Personnel and payroll systems are centrally located; there are plans to migrate the student information system to a central location.	Paper records are dispersed among program offices Electronic systems are at the Lili'uokalani Bldg., Kapolei, ICSD DHRD, and Arizona	Dispersed
13. <i>How does the agency dispose of physical and electronic records containing personal information?</i>	Disposal of personal information is decentralized and left to the discretion of offices and schools.	Hard drives are scrubbed or crushed, shredding in-house or by contractor.	
<i>Other comments</i>	DOE is the tenth largest school district in the country with 285 schools, 179,000 students,		

Questions	Department of Education	Department of Human Services	Department of Health
	20,552 regular employees and 23, 149 casual and part time employees; Other laws – FERPA (Family Educational Rights and Privacy Act)		

<i>Questions</i>	Bureau of Conveyances, Dept. of Land and Natural Resources		
<i>1. Kinds of personal information collected and stored</i>	Documents with personal information are primarily judgments and child support enforcement orders.		
<i>2. Number of records containing personal information</i>	Unknown. The Bureau was established in the 1800s and currently accepts 2,000 documents per day. Judgments and child support enforcement orders make up from 10 to 60% of the daily intake.		
<i>3. Is personal information made available to third parties?</i>	Yes. Currently, redaction is done on a piecemeal basis. The Bureau is working on a uniform policy.		
<i>4. What policies and practices related to internal and external access and security of the information?</i>			
<i>5. Is there one overall manager responsible for access and security within the agency or is responsibility dispersed?</i>	The First Deputy has overall responsibility.		
<i>6. Has there been any unauthorized access to personal information over the past several years?</i>			
<i>7. What training on confidentiality and handling of personal information is provided to staff?</i>	No formal training.		

Questions	Bureau of Conveyances, Dept. of Land and Natural Resources		
<i>8. What is the agency's most critical need to assure security of personal information?</i>	A method to handle past documents, cost of equipment, and manpower. Older records do not have Social Security numbers. Records prior to 1976 are on microfilm. Title companies and some attorneys have access to the Bureau's system.		
<i>9. What steps has the agency taken to comply with HRS Ch. 487J, 487N, and 487R?</i>			
<i>10. Are there any physical or electronic based solutions in place to protect personal information?</i>	The Bureau has been meeting with consultants.		
<i>11. Are there plans for any physical or electronic based solutions to protect personal information?</i>			
<i>12. Are the systems that contain personal information in one site or dispersed?</i>	Dispersed. Multiple copies are located at the archives and in storage. Title companies and law firms have copies.		
<i>13. How does the agency dispose of physical and electronic records containing personal information?</i>	Records are never disposed or destroyed.		
<i>Other comments.</i>	The law requires the Bureau to accept all documents for recordation.		

Exhibit 1. Personal Information Questionnaire

PERSONAL INFORMATION QUESTIONNAIRE

Purpose

The purpose of this questionnaire is to gather information on uses/disclosures of personal information by government agencies and the means deployed to secure the personal information from security breaches. The information collected will be used to perform a risk analysis of State and county agencies based on volume of personal information collected and maintained and the risk and impact of disclosure. Findings from the risk analysis will be prepared in a report to the State Legislature by the Identify Theft Task Force pertaining to implementation of HRS §487J (Social Security Number Protection), HRS §487N (Notice of Security Breach), and HRS §487R (Destruction of Personal Information Records).

Instructions

1. All government agencies (State and county) must complete the questionnaire. Government agencies may elect to:
 - a. Complete a single questionnaire representing responses from the entire agency (including administratively assigned agencies) or
 - b. Complete multiple questionnaires representing responses from each major subunit within the agency. A summary of multiple questionnaires must result in an accurate description of the policies/procedures/practices of the entire agency. All questionnaires representing the agency should be bundled together and submitted at the same time.
2. The expertise of more than one person may be needed to complete the questionnaire, depending upon the respondent's familiarity with current processes, policies and procedures within the unit. The survey may be completed by management, management in conjunction with appropriate personnel, or by delegating questions to subject matter experts.
3. Please respond to each question and sub-questions when applicable by placing an "X" in the appropriate YES or NO box. If the question is not applicable to your unit, enter a comment as to why it does not apply.
4. The *Comments* column of the questionnaire is used to ask the respondent to further clarify the answer beyond the standard YES or NO response.
5. An Addendum page is provided for extended responses to questionnaire items.
6. A glossary of terms is attached at the back of the questionnaire to ensure a common understanding of terms throughout the document and between respondents.
7. A Microsoft Word version of the questionnaire can be downloaded from the Office of the Auditor website at <http://www.state.hi.us/auditor/meetings.htm>
8. Questions on the questionnaire may be directed to Mr. Jeffrey Loo at (808) 528-7176 or jeffrey@jwlooassoc.com.
9. Completed questionnaire forms must be submitted to the State of Hawai'i, Office of the Auditor, 465 S. King Street, Room 500, Honolulu, HI 96813-2917 (Attention: Mr. Russell Wong) no later than January 31, 2007. Electronic copies of completed questionnaires may be transmitted to the Office of the Auditor at survey@auditor.state.hi.us.

Questionnaire Response For:		
Department Name:	Division/Branch:	Unit/Council/Board:
Contact Name:	Contact Telephone No.	Contact Email:
Authorized Agency Official Signature:	Date:	Questionnaire Completed for: <input type="checkbox"/> Entire Agency <input type="checkbox"/> Agency Subpart (other agency units completed separately)

1	Personal Information General Description
1A	List all types of documents/records (hard copy and electronic) containing personal information (e.g., applications, eligibility/enrollment records, medical records, employee/student/client files, licenses, authorization/consents, surveys/questionnaires, service payment claims, tax, real property conveyance, credit cards, judicial/law enforcement, etc.) that is handled, processed, or stored within your agency .
1B	What are the primary uses/purposes of the personal information (e.g., eligibility, case management, program payment/management, operational data analysis, fraud or abuse detection, data reporting, oversight or audit of programs/licenses, research, delivery of program services, law enforcement, judicial proceedings, legal recordation, etc.)? Please list.
1C	Who in your agency has access to the personal information maintained and what information is available? List the titles and /or categories of personnel who have <u>any</u> type of access to personal information (e.g., clerical staff, intake or eligibility workers, analysts, case managers, information technology staff, payments processing personnel, program staff, management, pool personnel, after-hours security service, janitorial service, couriers, etc.)
1D	<p>What is the estimated volume of individual records containing personal information maintained by your agency?</p> <p><input type="checkbox"/> None <input type="checkbox"/> 1 – 100 <input type="checkbox"/> 101 – 1,000 <input type="checkbox"/> 1,001 – 10,000 <input type="checkbox"/> 10,001 – 100,000 <input type="checkbox"/> 100,001 – 500,000 <input type="checkbox"/> 501,000 – 1,000,000 <input type="checkbox"/> 1,000,001 or more</p> <p><i>Note:</i> The volume estimate should include active/archived records, employee/client records, correspondence, electronic/hard copy database, transactions/proceedings, and all other government records that contain personal information. A record that is maintained in hard copy and electronic form is considered 2 records.</p>
1E	<p>What is the estimated annual volume growth of individual records containing personal information maintained by your agency?</p> <p><input type="checkbox"/> None <input type="checkbox"/> 1% – 5% <input type="checkbox"/> 6% – 10% <input type="checkbox"/> 11% – 25% <input type="checkbox"/> 26% – 50% <input type="checkbox"/> 51% – 75% <input type="checkbox"/> 76% – 100%</p> <p><input type="checkbox"/> 100% or more</p>

Questions		Yes	No	Comments
2	<i>Social Security Numbers</i>			
2A	Does your agency use/disclose individual Social Security Numbers or use/disclose documents/records that contain Social Security Numbers?			If your response is NO, skip to Item 3A.
2B	During the course of business, does your agency communicate or otherwise make available to the general public an individual's entire Social Security Number.			If your response is YES, please describe the circumstances.
2C	During the course of business, does your agency print/embed an individual's entire Social Security Number on any card required for the individual to access services provided by the agency?			
2D	During the course of business, does your agency require individuals to transmit the individual's entire Social Security Number over the Internet?			If your response is YES, are secure Internet connections deployed or is the Social Security Number encrypted?
2E	During the course of business, does your agency require individuals to use the individual's entire Social Security Number to access an Internet website?			
2F	During the course of business, does your agency unit print an individual's entire Social Security Number on any materials that are mailed to the individual?			If your response is YES, please describe the circumstances and specify if the inclusion of a Social Security Number in documents is required by the individual, by State/federal law, or by court/judicial order.
2G	Does your agency sell, lease, trade, rent, or otherwise intentionally release individuals' Social Security Numbers to a third party?			If your response is YES, please describe the circumstances and provide an estimated volume and frequency.
3	<i>Personal Information Use/Disclosure</i>			
3A	Does your unit receive personal information from other units in the department?			If your response is YES, list the information exchanged and the source of the information received.

Questions		Yes	No	Comments
3B	Does your unit transmit personal information to other units in the department?			If your response is YES, list the information exchanged and to whom information is disclosed.
3C	Does your unit receive personal information from outside your organization?			If your response is YES, list the information exchanged and the source of the information received.
3D	Does your unit transmit personal information outside the organization?			If your response is YES, list the information exchanged and to whom information is disclosed.
3E	Does your unit limit the use or disclosure of personal information to only that which is necessary to carry out the intended purpose?			If your response is NO, what are the barriers to reducing the use or disclosure of personal information in your work function?
3F	Is personal information exchanged/transmitted to/from your unit by any of the following means?			If your response is YES, please describe the safeguards, if any, used to assure that the information can be accessed/viewed/heard only by authorized individuals.
3F.1	Telephone			
3F.2	Interactive Voice Response (IVR) System			
3F.3	Facsimile Machine			
3F.4	Email			
3F.5	Internet/Intranet Website			
3F.6	Dialup/Broadband/Network File Transfer			
3F.7	Snail Mail			
3F.8	Courier/Air Freight/Messenger Service			

Questions		Yes	No	Comments
3F.9	Other. (Please specify).			
4	<i>Personal Information De-identification and Encryption</i>			
4A	When transmitting information/documents in hard copy out of your unit, are there specific procedures applied for redacting or concealing personal information?			If your response is YES, please describe the specific procedures used. If your response is NO, please specify the barriers to redacting personal information in your work function.
4B	When personal information is transmitted electronically, are any technical safeguards (e.g. file encryption, SSL), used to protect the information from unauthorized access during transmission?			If your response is YES, please describe the specific technical safeguards used.
4C	When personal information is stored on portable computer devices (e.g. laptops, smart phones), and/or removable electronic data storage devices (e.g. floppy disks, CD-ROM, portable hard drives, USB drives) and is transported out of your unit facility, are any technical safeguards (e.g. passwords, encryption) used to protect the information from unauthorized access if the device is lost/stolen?			If your response is YES, please describe the specific technical safeguards used
5	<i>Agency Contracts</i>			
5A	Does your unit have written agreements (contracts) with organizations that perform services on your behalf and have access to personal information?			If your response is NO, skip to Item 6A.
5B	Do the contracts/agreements with business associates contain language addressing:			
5B.1	The allowed uses/disclosures of personal information and prohibited uses.			
5B.2	Required physical/system safeguards to prevent unauthorized uses/disclosures.			
5B.3	Required reporting in the event of unauthorized use/disclosure and/or security breaches.			
5B.4	Requirements to assure that agents/subcontractors to whom personal information is disclosed agree to the same conditions.			

Questions		Yes	No	Comments
5B.5	Requirements to return or appropriately dispose/destroy personal information at the conclusion of the contract.			
6	<i>Agency Workforce Policies</i>			
6A	Are there policies on workforce member use, handling and disclosure of personal information?			If your response is YES, please describe the policy and indicate if there are specific sanctions for violations of the policy.
6B	Do workforce members sign confidentiality agreements applicable to personal information that they may use/disclose as part of their job function?			
6C	Are there policies/procedures to assure that workforce member access to personal information is terminated (e.g. return of keys, access entry combinations changed, passwords deactivated) when the workforce member separates/terminates from employment?			If your response is YES, please describe the policies/procedures.
6D	Is training on the appropriate use/disclosure of personal information required for workforce members?			If your response is NO, skip to Item 6D below.
6D.1	Does the training program apply to all work force members who use/disclose personal information to carry out their work functions?			
6D.2	Does the training program apply to all newly hired workforce members?			
6D.3	Does the training program accommodate information updates when there are material changes to applicable guidelines/laws/statutes/administrative rules?			
6D.4	Does the unit retain written documentation (e.g. materials, dates, attendees) of training provided?			
6E	Is there a policy or memorandum that designates responsibility for handling security breach events involving personal information?			If your response is YES, please describe the policy.
7	<i>Agency Policies and Procedures</i>			
7A	Are there general policies or procedures about the appropriate and restricted handling, use, and disclosure of personal information?			If your response is YES, please describe the policies/procedures.

Questions		Yes	No	Comments
7B	Are there policies or procedures requiring that personal information is secured and that stipulate the manner that is used to safeguard the information?			If your response is YES, please describe the policies/procedures.
7C	Are there policies or procedures for restricting the use/disclosure of personal information to a need to know basis?			If your response is YES, please describe the policies/procedures.
7D	Are there policies or procedures to verify the identity of individuals requesting access to personal information, if they are not known?			If your response is YES, please describe the policies/procedures.
7E	Are there policies or procedures that stipulate the conditions for secure storage/retention of personal information?			If your response is YES, please describe the policies/procedures.
7F	Are there policies or procedures that stipulate the conditions for secure disposal of personal information?			If your response is YES, please describe the policies/procedures.
7G	Are there policies or procedures that support the capability to identify personal information records contained in data/document files that are stored on portable computer and data storage devices in case they are lost/stolen?			If your response is YES, please describe the policies/procedures.
8	Agency Compliance			
8A	Has your agency unit initiated actions to comply with HRS §487J as it pertains to restricted use/disclosure of an individual's Social Security Number?			If your response is YES, please describe the actions taken to date.
8B	Does your agency unit expect to be in compliance with HRS §487J by July 1, 2007?			If your response is YES, please describe your procedures for performing required notifications. If you response is NO, please specify the significant barriers to compliance.
8C	Has your agency unit initiated actions to comply with HRS §487N as it pertains to performing notices of security breaches.			If your response is YES, please describe the actions taken to date.

Questions		Yes	No	Comments
8D	Does your agency unit expect to be in compliance with HRS §487N by January 1, 2007?			If your response is YES, please describe your procedures for performing required notifications. If you response is NO, please specify the significant barriers to compliance.
8E	Has your agency unit initiated actions to comply with HRS §487R as it pertains to destruction of personal information records?			If your response is YES, please describe the actions taken to date.
8F	Does your agency unit expect to be in compliance with HRS §487R by January 1, 2007?			If your response is YES, please describe your procedures for performing required notifications and the measures that will be used to assure the proper destruction/disposal of personal identifying information. If you response is NO, please specify the significant barriers to compliance.
8G	During 2006, did your agency unit have security breach events involving personal information?			If your response is YES, please specify the number and general circumstances of the security breach events. Also provide the estimated number of personal information records involved.

Addendum

Department Name:	Division/Branch:	Unit/Council/Board:
<i>Item No.</i>	<i>Comment</i>	

Glossary

<i>Term</i>	<i>Definition</i>
Business Associate	A person or organization that performs a function or activity on behalf of an agency unit but is not part of the entity's workforce. <i>45 CFR 160.103</i>
Encryption	The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. <i>HRS §487N-1</i>
Government Agency	Any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county. <i>HRS §487N-1</i>
Personal Information	<p>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:</p> <ol style="list-style-type: none"> 1. Social security number; 2. Driver's license number or Hawaii identification card number; or 3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account. (Note: Includes credit cards issued to employees for agency purchase purposes). <p>Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. <i>HRS §487N-1</i></p>
Records	Any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics. <i>HRS §487N-1</i>
Redacted	The rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data. <i>HRS §487N-1</i>
Security Breach	An incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. <i>HRS §487N-1</i>
Use	The sharing, employment, application, utilization, examination, or analysis of specified personal information within an agency unit that maintains such information. <i>45 CFR 164.501</i>
Workforce	Employees, volunteers, trainees, and other persons under the direct control of an agency unit. <i>45 CFR 160.103</i>

Exhibit 2. California Business and Professions Code, Section 350-352

350. (a) There is hereby created in the Department of Consumer Affairs an Office of Privacy Protection under the direction of the Director of Consumer Affairs and the Secretary of the State and Consumer Services Agency. The office's purpose shall be protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices in adherence with the Information Practices Act of 1977 (Chapter 1 (commencing with Section 1798) of Title 1.8 of Part 4 of Division 3 of the Civil Code).

(b) The office shall inform the public of potential options for protecting the privacy of, and avoiding the misuse of, personal information.

(c) The office shall make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers.

(d) The office may promote voluntary and mutually agreed upon nonbinding arbitration and mediation of privacy-related disputes where appropriate.

(e) The Director of Consumer Affairs shall do all of the following:

(1) Receive complaints from individuals concerning any person obtaining, compiling, maintaining, using, disclosing, or disposing of personal information in a manner that may be potentially unlawful or violate a stated privacy policy relating to that individual, and provide advice, information, and referral, where available.

(2) Provide information to consumers on effective ways of handling complaints that involve violations of privacy-related laws, including identity theft and identity fraud. If appropriate local, state, or federal agencies are available to assist consumers with those complaints, the director shall refer those complaints to those agencies.

(3) Develop information and educational programs and materials to foster public understanding and recognition of the purposes of this article.

(4) Investigate and assist in the prosecution of identity theft and other privacy-related crimes, and, as necessary, coordinate with local, state, and federal law enforcement agencies in the investigation of similar crimes.

(5) Assist and coordinate in the training of local, state, and federal law enforcement agencies regarding identity theft and other privacy-related crimes, as appropriate.

(6) The authority of the office, the director, or the secretary, to adopt regulations under this article shall be limited exclusively to those regulations necessary and appropriate to implement subdivisions (b), (c), (d), and (e).

352. (a) Subject to subdivision (b), the department shall commence activities under this article no later than January 1, 2002.

(b) The provisions of this article shall only be operative for those years in which there is an appropriation from the General Fund in the Budget Act to fund the activities required by this article.

(c) Funding sources other than the General Fund may be used to support this activity.

Exhibit 3. Missouri Revised Statutes, Chapter 59, County Recorders of Deeds, Section 59.331

August 28, 2007

Certain personal identifying information not to be included in certain documents for recording, exceptions.

59.331. The preparer of a document shall not include an individual's sensitive personal identifying information in a document that is prepared and presented for recording in the office of the recorder of deeds. "Sensitive personal identifying information" includes federal Social Security numbers, bank account numbers, and credit card account numbers. This section does not apply to state or federal tax liens, military separation or discharge papers, and other documents required by law to contain such information that are filed or recorded in the office of the recorder of deeds. Should any person's sensitive personal identifying information appear on any document prepared or submitted for recording, the preparer, submitter, or anyone in an agency relationship with the person may redact, remove, or delete the sensitive personal identifying information before submission to the recorder of deeds. Any such redaction, removal, or deletion shall not in any way affect the legal status of the transaction described in the document. The recorder of deeds shall not alter or modify any document in the official record except as otherwise provided by law.

(L. 2004 H.B. 795, et al., A.L. 2006 S.B. 932)

Exhibit 4. California Codes, Civil Code Section 1798-1798.1

1798. This chapter shall be known and may be cited as the Information Practices Act of 1977.

1798.1. The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:

(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

(c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

1798.3. As used in this chapter:

(a) The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

(b) The term "agency" means every state office, officer, department, division, bureau, board, commission, or other state agency, except that the term agency shall not include:

(1) The California Legislature.

(2) Any agency established under Article VI of the California Constitution.

(3) The State Compensation Insurance Fund, except as to any records which contain personal information about the employees of the State Compensation Insurance Fund.

(4) A local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

(c) The term "disclose" means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

(d) The term "individual" means a natural person.

(e) The term "maintain" includes maintain, acquire, use, or disclose.

(f) The term "person" means any natural person, corporation, partnership, limited liability company, firm, or association.

(g) The term "record" means any file or grouping of information about an individual that is maintained by an agency by reference to an identifying particular such as the individual's name, photograph, finger or voice print, or a number or symbol assigned to the individual.

(h) The term "system of records" means one or more records, which pertain to one or more individuals, which is maintained by any agency, from which information is retrieved by the name of an individual or by some identifying number, symbol or other identifying particular assigned to the individual.

(i) The term "governmental entity," except as used in Section 1798.26, means any branch of the federal government or of the local government.

(j) The term "commercial purpose" means any purpose which has financial gain as a major objective. It does not include the gathering or dissemination of newsworthy facts by a publisher or broadcaster.

(k) The term "regulatory agency" means the Department of Financial Institutions, the Department of Corporations, the Department of Insurance, the Department of Real Estate, and agencies of the United States or of any other state responsible for regulating financial institutions.

1798.14. Each agency shall maintain in its records only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.

1798.15. Each agency shall collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source.

1798.16. (a) Whenever an agency collects personal information, the agency shall maintain the source or sources of the information, unless the source is the data subject or he or she has received a copy of the source document, including, but not limited to, the name of any source who is an individual acting in his or her own private or individual capacity. If the source is an agency, governmental entity or other organization, such as a corporation or association, this requirement can be met by maintaining the name of the agency, governmental entity, or organization, as long as the smallest reasonably identifiable unit of that agency, governmental entity, or organization is named.

(b) On or after July 1, 2001, unless otherwise authorized by the Department of Information Technology pursuant to Executive Order D-3-99, whenever an agency electronically collects personal information, as defined by Section 11015.5 of the Government Code, the agency shall retain the source or sources or any intermediate form of the information, if either are created or possessed by the agency, unless the source is the data subject that has requested that the information be discarded or the data subject has received a copy of the source document.

(c) The agency shall maintain the source or sources of the information in a readily accessible form so as to be able to provide it to the data subject when they inspect any record pursuant to Section 1798.34. This section shall not apply if the source or sources are exempt from disclosure under the provisions of this chapter.

1798.17. Each agency shall provide on or with any form used to collect personal information from individuals the notice specified in this section. When contact with the individual is of a regularly recurring nature, an initial notice followed by a periodic notice of not more than one-year intervals shall satisfy this requirement. This requirement is also satisfied by notification to individuals of the availability of the notice in annual tax-related pamphlets or booklets provided for them. The notice shall include all of the following:

(a) The name of the agency and the division within the agency that is requesting the information.

(b) The title, business address, and telephone number of the agency official who is responsible for the system of records and who shall, upon request, inform an individual regarding the location of his or her records and the categories of any persons who use the information in those records.

(c) The authority, whether granted by statute, regulation, or executive order which authorizes the maintenance of the information.

(d) With respect to each item of information, whether submission of such information is mandatory or voluntary.

(e) The consequences, if any, of not providing all or any part of the requested information.

(f) The principal purpose or purposes within the agency for which the information is to be used.

(g) Any known or foreseeable disclosures which may be made of the information pursuant to subdivision (e) or (f) of Section 1798.24.

(h) The individual's right of access to records containing personal information which are maintained by the agency.

This section does not apply to any enforcement document issued by an employee of a law enforcement agency in the performance of his or her duties wherein the violator is provided an exact copy of the document, or to accident reports whereby the parties of interest may obtain a copy of the report pursuant to Section 20012 of the Vehicle Code.

The notice required by this section does not apply to agency requirements for an individual to provide his or her name, identifying number, photograph, address, or similar identifying information, if this information is used only for the purpose of identification and communication with the individual by the agency, except that requirements for an individual's social security number shall conform with the provisions of the Federal Privacy Act of 1974 (Public Law 93-579).

1798.18. Each agency shall maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness. Such standard need not be met except when such records are used to make any determination about the individual. When an agency transfers a record outside of state government, it shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely.

1798.19. Each agency when it provides by contract for the operation or maintenance of records containing personal information to accomplish an agency function, shall cause, consistent with its authority, the requirements of this chapter to be applied to those records. For purposes of Article 10 (commencing with Section 1798.55), any contractor and any employee of the contractor, if the contract is agreed to on or after July 1, 1978, shall be considered to be an employee of an agency. Local government functions mandated by the state are not deemed agency functions within the meaning of this section.

1798.20. Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.

1798.21. Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.

1798.22. Each agency shall designate an agency employee to be responsible for ensuring that the agency complies with all of the provisions of this chapter.

1798.23. The Department of Justice shall review all personal information in its possession every five years commencing July 1, 1978, to determine whether it should continue to be exempt from access pursuant to Section 1798.40.

1798.24. No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed, as follows:

(a) To the individual to whom the information pertains.

(b) With the prior written voluntary consent of the individual to whom the record pertains, but only if that consent has been obtained not more than 30 days before the disclosure, or in the time limit agreed to by the individual in the written consent.

(c) To the duly appointed guardian or conservator of the individual or a person representing the individual if it can be proven with reasonable certainty through the possession of agency forms, documents or correspondence that this person is the authorized representative of the individual to whom the information pertains.

(d) To those officers, employees, attorneys, agents, or volunteers of the agency that has custody of the information if the disclosure is relevant and necessary in the ordinary course of the performance of their official duties and is related to the purpose for which the information was acquired.

(e) To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which

the information was collected and the use or transfer is accounted for in accordance with Section 1798.25. With respect to information transferred from a law enforcement or regulatory agency, or information transferred to another law enforcement or regulatory agency, a use is compatible if the use of the information requested is needed in an investigation of unlawful activity under the jurisdiction of the requesting agency or for licensing, certification, or regulatory purposes by that agency.

(f) To a governmental entity when required by state or federal law.

(g) Pursuant to the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(h) To a person who has provided the agency with advance, adequate written assurance that the information will be used solely for statistical research or reporting purposes, but only if the information to be disclosed is in a form that will not identify any individual.

(i) Pursuant to a determination by the agency that maintains information that compelling circumstances exist that affect the health or safety of an individual, if upon the disclosure notification is transmitted to the individual to whom the information pertains at his or her last known address. Disclosure shall not be made if it is in conflict with other state or federal laws.

(j) To the State Archives as a record that has sufficient historical or other value to warrant its continued preservation by the California state government, or for evaluation by the Director of General Services or his or her designee to determine whether the record has further administrative, legal, or fiscal value.

(k) To any person pursuant to a subpoena, court order, or other compulsory legal process if, before the disclosure, the agency reasonably attempts to notify the individual to whom the record pertains, and if the notification is not prohibited by law.

(l) To any person pursuant to a search warrant.

(m) Pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code.

(n) For the sole purpose of verifying and paying government health care service claims made pursuant to Division 9 (commencing with Section 10000) of the Welfare and Institutions Code.

(o) To a law enforcement or regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

(p) To another person or governmental organization to the extent necessary to obtain information from the person or governmental organization as necessary for an investigation by the agency of a failure to comply with a specific state law that the agency is responsible for enforcing.

(q) To an adopted person and is limited to general background information pertaining to the adopted person's natural parents, provided that the information does not include or reveal the identity of the natural parents.

(r) To a child or a grandchild of an adopted person and disclosure is limited to medically necessary information pertaining to the adopted person's natural parents. However, the information, or the process for obtaining the information, shall not include or reveal the identity of the natural parents. The State Department of Social Services shall adopt regulations governing the release of information pursuant to this subdivision by July 1, 1985. The regulations shall require licensed adoption agencies to provide the same services provided by the department as established by this subdivision.

(s) To a committee of the Legislature or to a Member of the Legislature, or his or her staff when authorized in writing by the member, where the member has permission to obtain the information from the individual to whom it pertains or where the member provides reasonable assurance that he or she is acting on behalf of the individual.

(t) (1) To the University of California or a nonprofit educational institution conducting scientific research, provided the request for information is approved by the Committee for the Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CHHSA). The CPHS approval required under this subdivision shall include a review and determination that all the following criteria have been satisfied:

(A) The researcher has provided a plan sufficient to protect personal information from improper use and disclosures, including sufficient administrative, physical, and technical safeguards to protect personal information from reasonable anticipated threats to the security or confidentiality of the information.

(B) The researcher has provided a sufficient plan to destroy or return all personal information as soon as it is no longer needed for the research project, unless the researcher has demonstrated an ongoing need for the personal information for the research project and has provided a long-term plan sufficient to protect the confidentiality of that information.

(C) The researcher has provided sufficient written assurances that the personal information will not be reused or disclosed to any other person or entity, or used in any manner, not approved in the research protocol, except as required by law or for authorized oversight of the research project.

(2) The CPHS shall, at a minimum, accomplish all of the following as part of its review and approval of the research project for the purpose of protecting personal information held in agency databases:

(A) Determine whether the requested personal information is needed to conduct the research.

(B) Permit access to personal information only if it is needed for the research project.

(C) Permit access only to the minimum necessary personal information needed for the research project.

(D) Require the assignment of unique subject codes that are not derived from personal information in lieu of social security numbers if the research can still be conducted without social security numbers.

(E) If feasible, and if cost, time, and technical expertise permit, require the agency to conduct a portion of the data processing for the researcher to minimize the release of personal information.

(3) Reasonable costs to the agency associated with the agency's process of protecting personal information under the conditions of CPHS approval may be billed to the researcher, including, but not limited to, the agency's costs for conducting a portion of the data processing for the researcher, removing personal information, encrypting or otherwise securing personal information, or assigning subject codes.

(4) The CPHS may enter into written agreements to enable other institutional review boards to provide the data security approvals required by this subdivision, provided the data security requirements set forth in this subdivision are satisfied.

(u) To an insurer if authorized by Chapter 5 (commencing with Section 10900) of Division 4 of the Vehicle Code.

(v) Pursuant to Section 1909, 8009, or 18396 of the Financial Code.

This article shall not be construed to require the disclosure of personal information to the individual to whom the information pertains when that information may otherwise be withheld as set forth in Section 1798.40.

1798.24a. Notwithstanding Section 1798.24, information may be disclosed to any city, county, city and county, or district, or any officer or official thereof, if a written request is made to a local law enforcement agency and the information is needed to assist in the screening of a prospective concessionaire, and any affiliate or associate thereof, as these terms are defined in subdivision (k) of Section 432.7 of the Labor Code for purposes of consenting to, or approving of, the prospective concessionaire's application for, or acquisition of, any beneficial interest in a concession, lease, or other property interest. However, any summary criminal history information that may be disclosed pursuant to this section shall be limited to information pertaining to criminal convictions.

1798.24b. (a) Notwithstanding Section 1798.24, except subdivision (v) thereof, information shall be disclosed to the protection and advocacy agency designated by the Governor in this state pursuant to federal law to protect and advocate for the rights of people with disabilities, as described in Division 4.7 (commencing with Section 4900) of the Welfare and Institutions Code.

(b) Information that shall be disclosed pursuant to this section includes all of the following information:

- (1) Name.
- (2) Address.
- (3) Telephone number.
- (4) Any other information necessary to identify that person whose consent is necessary for either of the following purposes:
 - (A) To enable the protection and advocacy agency to exercise its authority and investigate incidents of abuse or neglect of people with disabilities.
 - (B) To obtain access to records pursuant to Section 4903 of the Welfare and Institutions Code.

1798.25. Each agency shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made pursuant to subdivision (j), (k), (l), (o), or (p) of Section 1798.24. This accounting shall also be required for disclosures made pursuant to subdivision (e) or (f) of Section 1798.24 unless notice of the type of disclosure has been provided pursuant to Sections 1798.9 and 1798.10. The accounting shall also include the name, title, and business address of the person or agency to whom the disclosure was made. For the purpose of an accounting of a disclosure made under subdivision (o) of Section 1798.24, it shall be sufficient for a law enforcement or regulatory agency to record the date of disclosure, the law enforcement or regulatory agency requesting the disclosure, and whether the purpose of the disclosure is for an investigation of unlawful activity under the jurisdiction of the requesting agency, or for licensing, certification, or regulatory purposes by that agency.

Routine disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement or regulatory agencies of federal, state, and local government shall be deemed to be disclosures pursuant to subdivision (e) of Section 1798.24 for the purpose of meeting this requirement.

1798.26. With respect to the sale of information concerning the registration of any vehicle or the sale of information from the files of drivers' licenses, the Department of Motor Vehicles shall, by regulation, establish administrative procedures under which any person making a request for information shall be required to identify himself or herself and state the reason for making the request. These procedures shall provide for the verification of the name and address of the person making a request for the information and the department may require the person to produce the information as it determines is necessary in order to ensure that the name and address of the person are his or her true name and address. These procedures may provide for a 10-day delay in the release of the requested information. These procedures shall also provide for notification to the person to whom the information primarily relates, as to what information was provided and to whom it was provided. The department shall, by regulation, establish a reasonable period of time for which a record of all the foregoing shall be maintained.

The procedures required by this subdivision do not apply to any governmental entity, any person who has applied for and has been issued a requester code by the department, or any court of competent jurisdiction.

1798.27. Each agency shall retain the accounting made pursuant to Section 1798.25 for at least three years after the disclosure for which the accounting is made, or until the record is destroyed, whichever is shorter. Nothing in this section shall be construed to require retention of the original documents for a three-year period, providing that the agency can otherwise comply with the requirements of this section.

1798.28. Each agency, after July 1, 1978, shall inform any person or agency to whom a record containing personal information has been disclosed during the preceding three years of any correction of an error or notation of dispute made pursuant to Sections 1798.35 and 1798.36 if (1) an accounting of the disclosure is required by Section 1798.25 or 1798.26, and the accounting has not been destroyed pursuant to Section 1798.27, or (2) the information provides the name of the person or agency to whom the disclosure was made, or (3) the person who is the subject of the disclosed record provides the name of the person or agency to whom the information was disclosed.

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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.

(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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) 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.

(3) Substitute notice, 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 all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.30. Each agency shall either adopt regulations or publish guidelines specifying procedures to be followed in order fully to implement each of the rights of individuals set forth in this article.

1798.32. Each individual shall have the right to inquire and be notified as to whether the agency maintains a record about himself or herself. Agencies shall take reasonable steps to assist individuals in making their requests sufficiently specific. Any notice sent to an individual which in any way indicates that the agency maintains any record concerning that individual shall include the title and business address of the agency official responsible for maintaining the records, the procedures to be followed to gain access to the records, and the procedures to be followed for an individual to contest the contents of these records unless the individual has received this notice from the agency during the past year. In implementing the right conferred by this section, an agency may specify in its rules or regulations reasonable times, places, and requirements for identifying an individual who requests access to a record, and for disclosing the contents of a record.

1798.33. Each agency may establish fees to be charged, if any, to an individual for making copies of a record. Such fees shall exclude the cost of any search for and review of the record, and shall not exceed ten cents (\$0.10) per page, unless the agency fee for copying is established by statute.

1798.34. (a) Except as otherwise provided in this chapter, each agency shall permit any individual upon request and proper identification to inspect all the personal information in any record containing personal information and maintained by reference to an identifying particular assigned to the individual within 30 days of the agency's receipt of the request for active records, and within 60 days of the agency's receipt of the request for records that are geographically dispersed or which are inactive and in central storage. Failure to respond within these time limits shall be deemed denial. In addition, the individual shall be permitted to inspect any personal information about himself or herself where it is maintained by reference to an identifying particular other than that of the individual, if the agency knows or should know that the information exists. The individual also shall be permitted to inspect the accounting made pursuant to Article 7 (commencing with Section 1798.25).

(b) The agency shall permit the individual, and, upon the individual's request, another person of the individual's own choosing to inspect all the personal information in the record and have an exact copy made of all or any portion thereof within 15 days of the inspection. It may require the individual to furnish a written statement authorizing disclosure of the individual's record to another person of the individual's choosing.

(c) The agency shall present the information in the record in a form reasonably comprehensible to the general public.

(d) Whenever an agency is unable to access a record by reference to name only, or when access by name only would impose an unreasonable administrative burden, it may require the individual to submit such other identifying information as will facilitate access to the record.

(e) When an individual is entitled under this chapter to gain access to the information in a record containing personal information, the information or a true copy thereof shall be made available to the individual at a location near the residence of the individual or by mail, whenever reasonable.

1798.35. Each agency shall permit an individual to request in writing an amendment of a record and, shall within 30 days of the date of receipt of such request:

(a) Make each correction in accordance with the individual's request of any portion of a record which the individual believes is not accurate, relevant, timely, or complete and inform the individual of the corrections made in accordance with their request; or

(b) Inform the individual of its refusal to amend the record in accordance with such individual's request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the head of the agency or an official specifically designated by the head of the agency of the refusal to amend, and the name, title, and business address of the reviewing official.

1798.36. Each agency shall permit any individual who disagrees with the refusal of the agency to amend a record to request a review of such refusal by the head of the agency or an official specifically designated by the head of such agency, and, not later than 30 days from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such review period by 30 days. If, after such review, the reviewing official refuses to amend the record in accordance with the request, the agency shall permit the individual to file with the agency a statement of reasonable length setting forth the reasons for the individual's disagreement.

1798.37. The agency, with respect to any disclosure containing information about which the individual has filed a statement of disagreement, shall clearly note any portion of the record which is disputed and make available copies of such individual's statement and copies of a concise statement of the reasons of the agency for not making the amendment to any person or agency to whom the disputed record has been or is disclosed.

1798.38. If information, including letters of recommendation, compiled for the purpose of determining suitability, eligibility, or qualifications for employment, advancement, renewal of appointment or promotion, status as adoptive parents, or for the receipt of state contracts, or for licensing purposes, was received with the promise or, prior to July 1, 1978, with the understanding that the identity of the source of the information would be held in confidence and the source is not in a supervisory position with respect to the individual to whom the record pertains, the agency shall fully inform the individual of all personal information about that individual without identification of the source. This may be done by providing a copy of the text of the material with only such deletions as are necessary to protect the identity of the source or by providing a comprehensive summary of the substance of the material. Whichever method is used, the agency shall insure that full disclosure is made to the subject of any personal information that could reasonably in any way reflect or convey anything detrimental, disparaging, or threatening to an individual's reputation, rights, benefits, privileges, or qualifications, or be used by an agency to make a determination that would affect an individual's rights, benefits, privileges, or qualifications. In institutions of higher education, "supervisory positions" shall not be deemed to include chairpersons of academic departments.

1798.39. Sections 1798.35, 1798.36, and 1798.37 shall not apply to any record evidencing property rights.

1798.40. This chapter shall not be construed to require an agency to disclose personal information to the individual to whom the information pertains, if the information meets any of the following criteria:

(a) Is compiled for the purpose of identifying individual criminal offenders and alleged offenders and consists only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status.

(b) Is compiled for the purpose of a criminal investigation of suspected criminal activities, including reports of informants and investigators, and associated with an identifiable individual.

(c) Is contained in any record which could identify an individual and which is compiled at any stage of the process of enforcement of the criminal laws, from the arrest or indictment stage through release from supervision and including the process of extradition or the exercise of executive clemency.

(d) Is maintained for the purpose of an investigation of an individual's fitness for licensure or public employment, or of a grievance or complaint, or a suspected civil offense, so long as the information is withheld only so as not to compromise the investigation, or a related investigation. The identities of individuals who provided information for the investigation may be withheld pursuant to Section 1798.38.

(e) Would compromise the objectivity or fairness of a competitive examination for appointment or promotion in public service, or to determine fitness for licensure, or to determine scholastic aptitude.

(f) Pertains to the physical or psychological condition of the individual, if the agency determines that disclosure would be detrimental to the individual. The information shall, upon the individual's written authorization, be disclosed to a licensed medical practitioner or psychologist designated by the individual.

(g) Relates to the settlement of claims for work related illnesses or injuries and is maintained exclusively by the State Compensation Insurance Fund.

(h) Is required by statute to be withheld from the individual to whom it pertains.

This section shall not be construed to deny an individual access to information relating to him or her if access is allowed by another statute or decisional law of this state.

1798.41. (a) Except as provided in subdivision (c), if the agency determines that information requested pursuant to Section 1798.34 is exempt from access, it shall inform the individual in writing of the agency's finding that disclosure is not required by law.

(b) Except as provided in subdivision (c), each agency shall conduct a review of its determination that particular information is exempt from access pursuant to Section 1798.40, within 30 days from the receipt of a request by an individual directly affected by the determination, and inform the individual in writing of the findings of the review. The review shall be conducted by the head of the agency or an official specifically designated by the head of the agency.

(c) If the agency believes that compliance with subdivision (a) would seriously interfere with attempts to apprehend persons who are wanted for committing a crime or attempts to prevent the commission of a crime or would endanger the life of an informant or other person submitting information contained in the record, it may petition the presiding judge of the superior court of the county in which the record is maintained to issue an ex parte order authorizing the agency to respond to the individual that no record is maintained. All proceedings before the court shall be in camera. If the presiding judge finds that there are reasonable grounds to believe that compliance with subdivision (a) will seriously interfere with attempts to apprehend persons who are wanted for committing a crime or attempts to prevent the commission of a crime or will endanger the life of an informant or other person submitting information contained in the record, the judge shall issue an order authorizing the agency to respond to the individual that no record is maintained by the agency. The order shall not be issued for longer than 30 days but can be renewed at 30-day intervals. If a request pursuant to this section is received after the expiration of the order, the agency must either respond pursuant to subdivision (a) or seek a new order pursuant to this subdivision.

1798.42. In disclosing information contained in a record to an individual, an agency shall not disclose any personal information relating to another individual which may be contained in the record. To comply with this section, an agency shall, in disclosing information, delete from disclosure such information as may be necessary. This section shall not be construed to authorize withholding the identities of sources except as provided in Sections 1798.38 and 1798.40.

1798.43. In disclosing information contained in a record to an individual, an agency need not disclose any information pertaining to that individual which is exempt under Section 1798.40. To comply with this section, an agency may, in disclosing personal information contained in a record, delete from the disclosure any exempt information.

1798.44. This article applies to the rights of an individual to whom personal information pertains and not to the authority or right of any other person, agency, other state governmental entity, or governmental entity to obtain this information.

1798.45. An individual may bring a civil action against an agency whenever such agency does any of the following:

(a) Refuses to comply with an individual's lawful request to inspect pursuant to subdivision (a) of Section 1798.34.

(b) Fails to maintain any record concerning any individual with such accuracy, relevancy, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, opportunities of, or benefits to the individual that may be made on the basis of such record, if, as a proximate result of such failure, a determination is made which is adverse to the individual.

(c) Fails to comply with any other provision of this chapter, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.

1798.46. In any suit brought under the provisions of subdivision (a) of Section 1798.45:

(a) The court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from the complainant. In such a suit the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld as being exempt from the individual's right of access and the burden is on the agency to sustain its action.

(b) The court shall assess against the agency reasonable attorney's fees and other litigation costs reasonably incurred in any suit under this section in which the complainant has prevailed. A party may be considered to have prevailed even though he or she does not prevail on all issues or against all parties.

1798.47. Any agency that fails to comply with any provision of this chapter may be enjoined by any court of competent jurisdiction. The court may make any order or judgment as may be necessary to prevent the use or employment by an agency of any practices which violate this chapter. Actions for injunction under this section may be prosecuted by the Attorney General, or any district attorney in this state, in the name of the people of the State of California whether upon his or her own complaint, or of a member of the general public, or by any individual acting in his or her own behalf.

1798.48. In any suit brought under the provisions of subdivision (b) or (c) of Section 1798.45, the agency shall be liable to the individual in an amount equal to the sum of:

(a) Actual damages sustained by the individual, including damages for mental suffering.

(b) The costs of the action together with reasonable attorney's fees as determined by the court.

1798.49. An action to enforce any liability created under Sections 1798.45 to 1798.48, inclusive, may be brought in any court of competent jurisdiction in the county in which the complainant resides, or has his principal place of business, or in which the defendant's records are situated, within two years from the date on which the cause of action arises, except that where a defendant has materially and willfully misrepresented any information required under this section to be disclosed to an individual who is the subject of the information and the information so misrepresented is material to the establishment of the defendant's liability to that individual under this section, the action may be brought at any time within two years after discovery by the complainant of the misrepresentation. Nothing in Sections 1798.45 to 1798.48, inclusive, shall be construed to authorize any civil action by reason of any injury sustained as the result of any information practice covered by this chapter prior to July 1, 1978. The rights and remedies set forth in this chapter shall be deemed to be nonexclusive and are in addition to all those rights and remedies which are otherwise available under any other provision of law.

1798.50. A civil action shall not lie under this article based upon an allegation that an opinion which is subjective in nature, as distinguished from a factual assertion, about an individual's qualifications, in connection with a personnel action concerning such an individual, was not accurate, relevant, timely, or complete.

1798.51. Where a remedy other than those provided in Articles 8 and 9 is provided by law but is not available because of lapse of time an individual may obtain a correction to a record under this

chapter but such correction shall not operate to revise or restore a right or remedy not provided by this chapter that has been barred because of lapse of time.

1798.53. Any person, other than an employee of the state or of a local government agency acting solely in his or her official capacity, who intentionally discloses information, not otherwise public, which they know or should reasonably know was obtained from personal information maintained by a state agency or from "records" within a "system of records" (as these terms are defined in the Federal Privacy Act of 1974 (P. L. 93-579; 5 U.S.C. 552a)) maintained by a federal government agency, shall be subject to a civil action, for invasion of privacy, by the individual to whom the information pertains. In any successful action brought under this section, the complainant, in addition to any special or general damages awarded, shall be awarded a minimum of two thousand five hundred dollars (\$2,500) in exemplary damages as well as attorney's fees and other litigation costs reasonably incurred in the suit. The right, remedy, and cause of action set forth in this section shall be nonexclusive and is in addition to all other rights, remedies, and causes of action for invasion of privacy, inherent in Section 1 of Article I of the California Constitution.

1798.55. The intentional violation of any provision of this chapter or of any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

1798.56. Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than five thousand dollars (\$5,000), or imprisoned not more than one year, or both.

1798.57. Except for disclosures which are otherwise required or permitted by law, the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of this chapter is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains. 1798.60. An individual's name and address may not be distributed for commercial purposes, sold, or rented by an agency unless such action is specifically authorized by law.

1798.61. (a) Nothing in this chapter shall prohibit the release of only names and addresses of persons possessing licenses to engage in professional occupations.

(b) Nothing in this chapter shall prohibit the release of only names and addresses of persons applying for licenses to engage in professional occupations for the sole purpose of providing those persons with informational materials relating to available professional educational materials or courses.

1798.62. Upon written request of any individual, any agency which maintains a mailing list shall remove the individual's name and address from such list, except that such agency need not remove the individual's name if such name is exclusively used by the agency to directly contact the individual.

1798.63. The provisions of this chapter shall be liberally construed so as to protect the rights of privacy arising under this chapter or under the Federal or State Constitution.

1798.64. (a) Each agency record which is accepted by the Director of General Services for storage, processing, and servicing in accordance with provisions of the State Administrative Manual for the purposes of this chapter shall be considered to be maintained by the agency which deposited the record and shall continue to be subject to the provisions of this chapter. The Director of General Services shall not disclose the record except to the agency which maintains the record, or pursuant to rules established by such agency which are not inconsistent with the provisions of this chapter.

(b) Each agency record pertaining to an identifiable individual which was or is transferred to the State Archives as a record which has sufficient historical or other value to warrant its continued preservation by the California state government, prior to or after July 1, 1978, shall, for the purposes of this chapter, be considered to be maintained by the archives.

1798.66. The time limits specified in Article 8 (commencing with Section 1798.30) may be extended to 60 days by the Franchise Tax Board if the following conditions exist:

- (a) The request is made during the period January 1 through June 30; and
- (b) The records requested are stored on magnetic tape.

1798.67. Where an agency has recorded a document creating a lien or encumbrance on real property in favor of the state, nothing herein shall prohibit any such agency from disclosing information relating to the identity of the person against whom such lien or encumbrance has been recorded for the purpose of distinguishing such person from another person bearing the same or a similar name.

1798.68. (a) Information which is permitted to be disclosed under the provisions of subdivision (e), (f), or (o), of Section 1798.24 shall be provided when requested by a district attorney. A district attorney may petition a court of competent jurisdiction to require disclosure of information when an agency fails or refuses to provide the requested information within 10 working days of a request. The court may require the agency to permit inspection unless the public interest or good cause in withholding such records clearly outweighs the public interest in disclosure.

(b) Disclosure of information to a district attorney under the provisions of this chapter shall effect no change in the status of the records under any other provision of law.

1798.69. (a) Except as provided in subdivision (b), the State Board of Equalization may not release the names and addresses of individuals who are registered with, or are holding licenses or permits issued by, the State Board of Equalization except to the extent necessary to verify resale certificates or to administer the tax and fee provisions of the Revenue and Taxation Code.

(b) Nothing in this section shall prohibit the release by the State Board of Equalization to, or limit the use by, any federal or state agency, or local government, of any data collected by the board that is otherwise authorized by law.

1798.70. This chapter shall be construed to supersede any other provision of state law, including Section 6253.5 of the Government Code, or any exemption in Section 6254 or 6255 of the Government Code, which authorizes any agency to withhold from an individual any record containing personal information which is otherwise accessible under the provisions of this chapter.

1798.71. This chapter shall not be deemed to abridge or limit the rights of litigants, including parties to administrative proceedings, under the laws, or case law, of discovery of this state.

1798.72. Nothing in this chapter shall be construed to authorize the disclosure of any record containing personal information, other than to the subject of such records, in violation of any other law.

1798.73. Nothing in this chapter shall be construed to deny or limit any right of privacy arising under Section 1 of Article I of the California Constitution.

1798.74. The provisions of Chapter 13 (commencing with Section 67110) of Part 40 of the Education Code shall, with regard to student records, prevail over the provisions of this chapter.

1798.75. This chapter shall not be deemed to supersede Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code, except as to the provisions of Sections 1798.60, 1798.69, and 1798.70.

1798.76. Nothing in this chapter shall be construed to revoke, modify, or alter in any manner any statutory provision or any judicial decision which (a) authorizes an individual to gain access to any law enforcement record, or (b) authorizes discovery in criminal or civil litigation.

1798.77. Each agency shall ensure that no record containing personal information shall be modified, transferred, or destroyed to avoid compliance with any of the provisions of this chapter. In the event that an agency fails to comply with the provisions of this section, an individual may bring a civil action and seek the appropriate remedies and damages in accordance with the provisions of Article 9 (commencing with Section 1798.45). An agency shall not remove or destroy personal information about an individual who has requested access to the information before allowing the individual access to the record containing the information.

1798.78. This chapter shall not be deemed to supersede the provisions of Chapter 1299 of the Statutes of 1976.

Exhibit 5. California Codes, Civil Code Section 1788.18

1788.18. (a) Upon receipt from a debtor of all of the following, a debt collector shall cease collection activities until completion of the review provided in subdivision (d):

(1) A copy of a police report filed by the debtor alleging that the debtor is the victim of an identity theft crime, including, but not limited to, a violation of Section 530.5 of the Penal Code, for the specific debt being collected by the debt collector.

(2) The debtor's written statement that the debtor claims to be the victim of identity theft with respect to the specific debt being collected by the debt collector.

(b) The written statement described in paragraph (2) of subdivision (a) shall consist of any of the following:

(1) A Federal Trade Commission's Affidavit of Identity Theft.

(2) A written statement containing the content of the Identity Theft Victim's Fraudulent Account Information Request offered to the public by the California Office of Privacy Protection.

(3) A written statement that certifies that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification. A person submitting the certification who declares as true any material matter pursuant to this subdivision that he or she knows to be false is guilty of a misdemeanor. The statement shall contain or be accompanied by, the following, to the extent that an item listed below is relevant to the debtor's allegation of identity theft with respect to the debt in question:

(A) A statement that the debtor is a victim of identity theft.

(B) A copy of the debtor's driver's license or identification card, as issued by the state.

(C) Any other identification document that supports the statement of identity theft.

(D) Specific facts supporting the claim of identity theft, if available.

(E) Any explanation showing that the debtor did not incur the debt.

(F) Any available correspondence disputing the debt after transaction information has been provided to the debtor.

(G) Documentation of the residence of the debtor at the time of the alleged debt. This may include copies of bills and statements, such as utility bills, tax statements, or other statements from businesses sent to the debtor, showing that the debtor lived at another residence at the time the debt was incurred.

(H) A telephone number for contacting the debtor concerning any additional information or questions, or direction that further communications to the debtor be in writing only, with the mailing address specified in the statement.

(I) To the extent the debtor has information concerning who may have incurred the debt, the identification of any person whom the debtor believes is responsible.

(J) An express statement that the debtor did not authorize the use of the debtor's name or personal information for incurring the debt.

(K) The certification required pursuant to this paragraph shall be sufficient if it is in substantially the following form:

"I certify the representations made are true, correct, and contain no material omissions of fact.

_____ "
(Date and Place)

(Signature)

(c) If a debtor notifies a debt collector orally that he or she is a victim of identity theft, the debt collector shall notify the debtor, orally or in writing, that the debtor's claim must be in writing. If a debtor notifies a debt collector in writing that he or she is a victim of identity theft, but omits information required pursuant to subdivision (a) or, if applicable, the certification required pursuant to paragraph (3) of subdivision (b), if the debt collector does not cease collection activities, the debt collector shall provide written notice to the debtor of the additional information

that is required, or the certification required pursuant to paragraph (3) of subdivision (b), as applicable or send the debtor a copy of the Federal Trade Commission's Affidavit of Identity Theft form.

(d) Upon receipt of the complete statement and information described in subdivision (a), the debt collector shall review and consider all of the information provided by the debtor and other information available to the debt collector in its file or from the creditor. The debt collector may recommence debt collection activities only upon making a good faith determination that the information does not establish that the debtor is not responsible for the specific debt in question. The debt collector's determination shall be made in a manner consistent with the provisions of 15 U.S.C. Sec. 1692f(1), as incorporated by Section 1788.17. The debt collector shall notify the debtor in writing of that determination and the basis for that determination before proceeding with any further collection activities. The debt collector's determination shall be based on all of the information provided by the debtor and other information available to the debt collector in its file or from the creditor.

(e) No inference or presumption that the debt is valid or invalid, or that the debtor is liable or not liable for the debt, shall arise if the debt collector decides after the review described in subdivision (d) to cease or recommence the debt collection activities. The exercise or nonexercise of rights under this section is not a waiver of any other right or defense of the debtor or debt collector.

(f) The statement and supporting documents that comply with subdivision (a) may also satisfy, to the extent those documents meet the requirements of, the notice requirement of paragraph (5) of subdivision (c) of Section 1798.93.

(g) A debt collector who ceases collection activities under this section and does not recommence those collection activities, shall do all of the following:

(1) If the debt collector has furnished adverse information to a consumer credit reporting agency, notify the agency to delete that information.

(2) Notify the creditor that debt collection activities have been terminated based upon the debtor's claim of identity theft.

(h) A debt collector who has possession of documents that the debtor is entitled to request from a creditor pursuant to Section 530.8 of the Penal Code is authorized to provide those documents to the debtor.

(i) Notwithstanding subdivision (h) of Section 1788.2, for the purposes of this section, "debtor" means a natural person, firm, association, organization, partnership, business trust, company, corporation, or limited liability company from which a debt collector seeks to collect a debt that is due and owing or alleged to be due and owing from the person or entity. The remedies provided by this title shall apply equally to violations of this section.

This page intentionally left blank