Report on Electronic Commerce-Based Crimes

Prepared by the
Hawaii Anti-Phishing Task Force
Pursuant to Act 65,
Session Laws of Hawaii 2005

Submitted to
The Twenty-Third Legislature
Regular Session of 2006

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW

Creation of the Task Force

The Hawaii Anti-Phishing Task Force (Task Force) was established in the Department of the Attorney General by Act 65, Session Laws of Hawaii 2005 (Act) to develop state policy on how best to prevent further occurrences of phishing and other forms of electronic commerce-based crimes in the State.

"Phishing" is a term used to describe Internet information-gathering schemes in which scammers attempt to dupe Internet users into divulging confidential information, such as credit card numbers, passwords, and account information, under false pretenses.[1] The victims of phishing are vulnerable to credit card fraud and identity theft.[2]

The Act directs the Task Force to:

(1) Examine the policies, procedures, and operations of state agencies charged with the responsibility of developing policies to prevent electronic commerce-based crimes, monitoring electronic commerce-based criminal activity, and enforcing electronic commerce-based criminal sanctions;

(2) Review other jurisdictions' activities, policies, directives, and laws related to preventing electronic commerce-based crimes and derive best practices models therefrom;

(3) Explore any other options available to the Task Force to deter electronic commerce-based crimes from occurring in the State; and

(4) Establish findings and develop recommendations on how the State may best deter electronic commerce-based crimes from occurring in the State.

The Act requires the Task Force to submit its findings and recommendations, including any proposed legislation, to the Legislature no later than twenty days before the start of the 2006 regular session.

---

[1] Act 65, SLH 2005. "Phishers" send millions of fake electronic mails that appear to come from popular websites or from sites Internet users trust, like a bank or credit card company. The electronic mails and website links that phishers send often look official enough to trick people into believing that the sites are legitimate. To make the electronic mails look more realistic, scam artists might put a link in the fake electronic mail that appears to go to a legitimate website, but actually takes an unsuspecting Internet user to a scam site or pop-up window that looks exactly like the official site. *Id*.

[2] *Id*.

The Task Force ceases to exist on June 30, 2006.

Task Force Members and Meetings

The Act specifies the composition of the Task Force. The eleven members are:

(1) The Attorney General or the Attorney General's designee (Supervising Deputy Attorney General Christopher D. W. Young);

(2) The Director of the Office of Consumer Protection (Stephen H. Levins);

(3) The United States Attorney for the District of Hawaii or the United States Attorney's designee (Assistant U.S. Attorney Ronald G. Johnson);

(4) Two members of the Hawaii State Senate appointed by the President of the Senate (Senator Carol Fukunaga and Senator Ron Menor);

(5) Two members of the Hawaii State House of Representatives appointed by the Speaker of the House of Representatives (Representative Colleen Meyer and Representative Brian Schatz);

(6) Two members representing the financial services industry, one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives (Marvin S. C. Dang, attorney for the Hawaii Financial Services Association, and Gary Caulfield, Vice Chair of First Hawaiian Bank);

(7) A member of the Honolulu Police Department's Criminal Investigation Division (Lt. Jeff Richards); and

(8) A member of the Honolulu field office's United States Secret Service electronic crimes unit (Special Agent Christian Roylo).

Support services were provided to the Task Force by Deputy Attorney General Kristin Izumi-Nitao, Legal Assistant Tracey Webb, and Legal Secretary Dyann Tonaki of the Department of the Attorney General, Juli Horka-Ruiz from the Senate Majority Research staff, and James Dixon from the Law Offices of Marvin Dang.

The Task Force first met on September 2, 2005, and held eight additional meetings. All meetings were open to the public.

The members elected Christopher Young as Chair. Gary Caulfield was elected Vice Chair.

Focus of the Task Force

The Task Force recognized that there is no uniform definition of the term "electronic commerce-based crimes" among law enforcement officials in Hawaii. For the purpose of the Task Force's work, the term "electronic commerce-based crimes" encompasses crimes and scams under the broader category of "identity theft" and those offenses committed as precursors to identity theft. Generally, identity theft means the unauthorized use of another person's confidential "personal information" to obtain credit, goods, services, money, or property, or to commit fraud.

There are many components of confidential "personal information." The Task Force noted that in the Hawaii Penal Code, "personal information" is defined as follows:

> "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.[3]

Theft of confidential personal information typically precedes the actual identity theft. These precursors range from stealing mail from an unlocked mailbox, to submitting a change of address form to divert mail to another location, to rummaging through trash in a practice known as "dumpster diving." Criminals obtain confidential personal information from businesses or other institutions by stealing records or information while on the job, conning or bribing an employee with access to records, hacking computer records, or abusing legitimate access to consumer credit reports. The Task Force learned that confidential personal information could be obtained legitimately from state government files and records, which lack adequate safeguards (such as redacting the confidential personal information).

Identity theft is a growing problem throughout the United States. In 2003, the Federal Trade Commission (FTC) received over half a million consumer fraud and identity theft complaints.[4] During 2004, the FTC received over 635,000 consumer fraud and identity theft complaints. Nationally, fraud-related consumer losses in 2004 totaled more than $547 million.[5]

---

[3] Haw. Rev. Stat. § 708-800.

[4] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2003" available on the Internet at http://www.ftc.gov/opa/2004/01/top10.htm.

[5] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2004" available on the internet at http://www.ftc.gov/opa/2005/02/top102005.htm.

According to FTC data, Hawaii ranked fifth highest in the nation for fraud complaints per 100,000 population unit in 2004. Hawaii consumers reported 1,807 fraud complaints, or 143.1 complaints per 100,000 population unit. It appears that a significant proportion of consumer complaints – thirty-nine percent – involved Internet auctions. Other fraud categories included shop-at-home and catalog sales, prizes or sweepstakes and lotteries, Internet services and computer complaints, and foreign money offers.[6]

During 2004, 640 Hawaii residents reported to the FTC that they were victims of identity theft, or 50.7 victims per 100,000 population unit, making Hawaii thirty-third in the nation for identity theft victims.[7] Credit card fraud was the most prevalent underlying identity theft crime. Other underlying crimes include phone or utilities fraud, bank fraud, government documents or benefits fraud, and loan fraud.[8]

By addressing the problem of the theft of confidential personal information, identity theft can be curtailed. Phishing is one method of stealing confidential personal information. However, for reporting purposes, complaints about phishing are grouped with identity theft complaints. What is known is that phishing is a relatively small part of the identity theft problem. Accurate statistics for identity theft and fraud activities are very difficult to obtain, because these crimes are under-reported to law enforcement authorities and because people sometimes do not know they have been victimized. The Task Force recognized that sufficient financial resources are needed to ensure the compilation of accurate statistics to know the full extent of the identity theft problem in Hawaii.

The Task Force was informed that many of the criminals operating phishing scams that victimize Hawaii residents are mass e-mailers located in Eastern Europe or the former Soviet Union. Similarly, many other Internet-based identity theft scams perpetuated against Hawaii residents are committed by people outside the State of Hawaii. For these reasons, the Task Force members agreed that it would be extremely difficult, if not impossible, for the State of Hawaii, acting alone, to take effective legal action against all phishing scams and all Internet-based fraud because of geographic distance and jurisdictional issues.

Besides high-tech activities such as phishing and Internet-based fraud, there are other types of identity theft committed against Hawaii residents involving very low-tech activities. Some of the perpetrators are close friends and family members who steal credit cards of the victim or use without authorization the victim's confidential personal information to obtain credit. Other types of low-tech activities in Hawaii by thieves seeking to obtain confidential personal information include stealing from mailboxes and "dumpster diving." The Task Force discussed ways in which the State could deter the low technology, non-electronic activities, which frequently precede electronic

---

[6] Federal Trade Commission, *National and State Trends in Fraud & Identity Theft, January - December 2004* available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf at p. 15 of 71.
[7] *Id.*
[8] *Id.* at p. 28 of 71.

commerce-based identity theft crimes in Hawaii. An important addition would be a Hawaii mail theft statute.

The Task Force heard how the use of crystal methamphetamine and other illegal drugs plays a part in both high-tech and low-tech identity theft activities in Hawaii. There is evidence of a relationship between the use and sale of illegal drugs and the theft of confidential personal information in Hawaii. Drug users have stolen mail to obtain confidential personal information, which they then sell for cash or drugs. Also, the Task Force learned that crystal methamphetamine users have been given drugs by identity thieves in exchange for reassembling shredded documents containing confidential personal information. The nexus between illegal drugs and identity theft deserves further investigation and study.

Combating identity theft in Hawaii requires coordinated action by all levels and branches of government and by the private sector. Public education plays an integral role. The creation of the Task Force enhances that effort. But much more work and resources are needed to protect Hawaii's people from identity theft and other electronic commerce-based crimes.

Organization of this Report

This Report is divided into four Sections. Each Section corresponds to the four activities that the Act requires that the Task Force accomplish.

SECTION 1

POLICIES, PROCEDURES AND OPERATIONS OF AGENCIES CHARGED WITH THE RESPONSIBILITY OF PREVENTING ELECTRONIC COMMERCE-BASED CRIMES, MONITORING ELECTRONIC COMMERCE-BASED CRIMINAL ACTIVITY, AND ENFORCING ELECTRONIC COMMERCE-BASED CRIMINAL SANCTIONS

Numerous governmental enforcement agencies in the State of Hawaii have adopted and implemented various strategies to address the increasing problem of identity theft. These include a myriad of county, state, and federal agencies, such as the county police departments, the county prosecuting attorneys, the State of Hawaii Department of the Attorney General, the State of Hawaii Department of Commerce and Consumer Affairs, the United States Attorney, the United States Postal Service, and the United States Secret Service.

County Police Departments

The various county police departments process identity theft cases on a daily basis. Although the nature and extent of investigation and enforcement varies widely, the critical factors faced by all include the availability and allocation of limited resources. Trained investigators must be assigned, sophisticated equipment must be utilized, and financial resources must be secured. Despite finite resources, however, every county police department recognizes identity theft as a growing problem that must be addressed. Law enforcement officers regularly arrest suspects for stealing checks, mail, credit cards, or confidential documents. Each of these types of cases constitutes a potential identity theft case. Although each police department sets its own priorities, and each would like to obtain additional resources to fight this growing problem, all pursue identity theft cases if the facts of an investigation warrant it.

Department of the Attorney General

The State of Hawaii Department of the Attorney General has recognized identity theft as a significant problem in Hawaii and has committed a substantial amount of resources to combat it.

In 2002, the department created the Hawaii High Technology Crime Unit (HHTCU) to increase investigations and prosecutions of computer-related crimes such as identity theft, computer damage, computer fraud, and unauthorized computer access. See sections 708-839 and 708-890, Hawaii Revised Statutes. Operationally, the department has worked very closely with almost every criminal law enforcement authority in Hawaii to fulfill its mission. In practice, the HHTCU has found that Internet fraud has become its focus.

On average, the HHTCU receives about sixty to seventy referrals each month from the Internet Crime Complaint Center (IC3) concerning Internet fraud. IC3 is an alliance between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation that provides victims with a mechanism for reporting fraud online and forwards that information to law enforcement and regulatory agencies as

appropriate. The HHTCU works these cases full-time with its primary objective being to recover money for the victims. As of late 2005, the unit has recovered approximately $200,000.

In an effort to achieve its goals, the HHTCU has set forth the following objectives: (1) increase the investigative capabilities of local law enforcement officers in the detection, investigation, and apprehension of computer related crimes through training; (2) increase the number of computer related cases being investigated by the State of Hawaii by providing and equipping its computer forensics lab with qualified examiners and technical support; (3) maintain the multi-agency task force response to computer related crimes in the State of Hawaii and increase participation; and (4) maintain and increase public awareness and prevention programs through Internet access and public education. Currently, two prosecutors, three investigators, and two computer forensic examiners, one of whom also serves as an educational liaison, staff the unit.

County Prosecuting Attorneys

The county prosecuting attorneys prosecute traditional economic crimes such as theft, forgery, credit card fraud, and identity theft. Many of these cases are brought pursuant to Hawaii's identity theft statute, section 708-839, Hawaii Revised Statutes.

In coordination and consultation with their local county police departments, the county prosecutors have prosecuted hundreds of identity theft cases during the past few years through the use of identity theft statutes as well as traditional theft statutes. Individuals convicted pursuant to these laws are subject to incarceration of up to ten years and a fine of up to $25,000.

Office of Consumer Protection

The Office of Consumer Protection (OCP) has civil enforcement authority pursuant to chapter 487, Hawaii Revised Statutes, to enforce Hawaii's consumer protection statutes. Functionally, this means that OCP has jurisdiction over a wide range of businesses and activities, including both regulated and unregulated industries. In the area of identity theft, OCP's focus has been on public education regarding prevention, reporting, and resolution. This past summer, OCP and the Department of Commerce and Consumer Affairs (DCCA) produced four public service announcements warning consumers regarding the dangers associated with identity theft. In conjunction with the public service announcements, DCCA created a website devoted to assisting consumers who have questions or concerns. The website can be found at: www.hawaii.gov/dcca/quicklinks/id_theft_info. Additionally, OCP has specially trained investigators who respond to telephone inquiries.

Federal Enforcement

There are a number of federal laws applicable to identity theft that may be used for the prosecution of identity theft offenses. Identity theft is often committed to facilitate other crimes, although it is frequently the primary goal of the offender. Schemes to commit identity theft may involve a number of other federal statutes including

identification fraud (18 U.S.C. § 1028(a)(1) - (6)), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), financial institution fraud (18 U.S.C. § 1344), mail theft (18 U.S.C. § 1708), and immigration document fraud (18 U.S.C. § 1546).

The primary identity theft statute, 18 U.S.C. § 1028(a)(7), was enacted on October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act (Identity Theft Act). The Identity Theft Act criminalizes fraud in connection with the unlawful theft and misuse of personal identifying information.

Recent amendments to the Identity Theft Act have enhanced its penalty provisions by applying more stringent penalties for identity thefts involving property offenses. It provides for a term of imprisonment of not more than fifteen years when an individual commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value aggregating $1,000 or more during any one-year period is obtained.

The Identity Theft Act also directed the Federal Trade Commission (FTC) to establish a procedure to log in and acknowledge receipt of complaints from victims of identity theft, to provide educational materials to these victims, and to refer the complaints to appropriate entities. The FTC has responded to this directive by developing a website, informative educational materials, a hotline for complaints, and a central database for information. The website can be found at www.consumer.gov/idtheft. The hotline is 1-877-ID-THEFT (1-877-438-4338). Identity theft complaints are entered into Consumer Sentinel, a secure, on-line database available to law enforcement. The FTC has become a primary referral point for victims of identity theft and a tremendous resource for these victims and law enforcement.

In 2004, Congress passed the Identity Theft Penalty Enhancement Act. This act creates a new class of federal crime, aggravated identity theft, defined as identity theft used in the commission of a felony. Convictions for aggravated identity theft carry a mandatory tack-on penalty of two years of incarceration. The act also orders the United States Sentencing Commission, which sets federal sentencing guidelines, to enhance penalties for company or government insiders who steal data that is then used in identity theft crimes.

The U.S. Secret Service was mandated by the PATRIOT Act to establish a nationwide network of Electronic Crimes Task Forces (ECTF). The concept of the ECTF is unique in that it brings together not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. The common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on our nation's financial and critical infrastructures. The priority of the ECTF is to focus on criminal activity that violates the aforementioned federal laws in which there is either a high dollar loss, large impact to the community, transnational or multi-district jurisdiction, or a new technology or scheme. The U.S. Secret Service Electronic Crimes Task Forces have grown from the initial Task Force in New York to fifteen Electronic

Crimes Task Forces and eight Electronic Crimes Working Groups spanning the entire nation.

Identity Theft and Fraud Task Force

In an effort to combat this problem, several law enforcement authorities in Hawaii recently came together to form a joint task force, known as the Identity Theft and Fraud Task Force.

The Identity Theft and Fraud Task Force or "Hit Fraud" Task Force was organized in October 2004 and consists of a group of state, federal, and county law enforcement officials, including the United States Attorney, the United States Postal Inspection Service, the Federal Bureau of Investigation, the United States Secret Service, the United States Bureau of Immigration and Customs Enforcement, the United States Marshals Service, the State of Hawaii Department of the Attorney General, the State of Hawaii Department of Commerce and Consumer Affairs, county police departments and county prosecutors' offices. The task force meets periodically to exchange information and to form and implement strategies designed to protect the public from this growing problem. One of its main goals is to enhance the prosecution of identity theft by targeting career criminals and the most egregious offenders through the use of federal fraud and identity theft laws. In this regard, prosecutors have been using the Identity Theft Penalty Enhancement Act of 2004 to facilitate prosecution. This recently enacted federal law allows the federal law enforcement authorities to seek a two-year mandatory term of incarceration in addition to any other sentence imposed for identity theft. It is anticipated that the enhanced sentencing provisions will help deter the proliferation of this crime in Hawaii.

As part of the task force, a United States postal inspector has been lodged within the Honolulu Police Department's financial fraud and white-collar crime unit for more than a year, offering expertise in sorting through the hundreds of fraud and identity theft cases and helping to identify those cases warranting federal prosecution.

While the task force's joint law enforcement initiative has been an effective tool in combating the problem, it is acknowledged that the primary jurisdiction of each law enforcement authority is of critical importance and remains the bulwark of the governments' efforts.

SECTION 2

REVIEW OF OTHER JURISDICTIONS' ACTIVITIES, POLICIES, DIRECTIVES, AND LAWS RELATED TO PREVENTING ELECTRONIC COMMERCE-BASED CRIMES TO DERIVE BEST PRACTICES MODELS THEREFROM.

CRIMINAL LAWS

This section encompasses a review of other jurisdictions' laws relating to preventing identity theft, phishing, and other electronic commerce-based crimes. A complete listing of state laws in the aforementioned areas is provided in Appendix I. A listing of legislation (civil and criminal) enacted in 2005 from the United States relating to the protection of personal information, computer crimes, identity theft, and other electronic based crimes, is provided in Appendix II.

State Identity Theft Statutes

Overview

At the outset, it is noteworthy that all states have some form of criminal law preventing identity theft. However, no two are alike. Therefore, for purposes of this discussion, we highlight some emerging themes that distinguish other jurisdictions' identity theft laws from our laws in the State of Hawaii.

First, many states define the act of identity theft as when a person uses another's personal identifying information for any unlawful purpose, including to obtain or attempt to obtain money, credit, goods, services, property, medical information, financial information, employment, or other benefit or any thing of value in another's name without his/her consent.[9] Although these jurisdictions share this language, the state of mind to commit this crime differs. Moreover, some laws are written more broadly to include not only obtaining or attempting to obtain another's personal identifying information, but also possessing another's personal identifying information for any unlawful purpose.[10] In some states, the criminal penalty or classification of the crime will depend on the financial or dollar loss sustained.[11]

Second, some states recognize that assuming another's identity or professing to be another to harm, deprive, defraud another to obtain money, credit, goods, services, or any thing of value without his/her consent constitutes identity theft.[12] Notably, in Indiana, it is not a defense that no person was actually harmed or defrauded.

---

[9] Examples of these, and related statutes, can be found in Appendix I (California, Connecticut, District of Columbia, Iowa, Louisiana, Maryland, Massachusetts, Michigan, Mississippi, Montana, Nevada, New Jersey, Oklahoma, Tennessee, Utah, Virginia, Washington, Wisconsin, and Wyoming).

[10] See, e.g., Appendix I (District of Columbia, Maryland, Tennessee, Washington, and Wisconsin).

[11] See, e.g., Appendix I (District of Columbia, Iowa, Louisiana, Maryland, Mississippi, Montana, New Jersey, Utah, Virginia, Washington, and Wyoming).

[12] Examples of these, and related statutes, can be found in Appendix I and Appendix II (Indiana, Kentucky, Maryland, Massachusetts, Michigan, Nebraska, New Hampshire, New Jersey, New York, and North Carolina).

Third, possession alone of another's personal identifying information without authorization and with intent to defraud or commit a crime or for any unlawful purpose constitutes an offense in some jurisdictions.[13] Missouri also makes it a criminal offense to traffic in stolen identifications and provides that possession of five or more identifications of the same person, or possession of identification of five or more separate persons, is evidence that these identifications are possessed with intent to manufacture, sell, or transfer identification for purposes of committing identity theft. In New Jersey, it is a criminal offense to fraudulently use, distribute, manufacture, or possess any item containing another's personal identifying information without his/her permission. If a person distributed, manufactured, or possessed twenty or more items containing another's personal identifying information without his/her authorization, or five or more items containing personal identifying information pertaining to five or more persons without their authorization, an inference is created that the items were distributed, manufactured, or possessed with knowledge that the actor is facilitating a fraud or an injury to be perpetrated.

Fourth, a few states consider obtaining or recording another's personal identifying information without consent in order to access another's financial resources as identity theft.[14]

Fifth, there are other states that have very broad language that makes identity theft a crime. For instance, in Arizona, a person who knowingly takes, purchases, manufactures, records, possesses, or uses any personal identifying information for any unlawful purpose or to cause loss, whether or not there is an actual economic loss, constitutes a felony crime of identity theft. In Florida, a person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, another's personal identifying information without consent, commits a felonious offense of fraudulent use of personal identification information. In New Mexico, it is unlawful to willfully obtain, record, or transfer personal identifying information of another without his/her consent and with intent to defraud. In Oregon, it is a felony to obtain, possess, transfer, create, utter, or convert to the person's own use the personal identifying information of another. Lastly, in Alabama, there are three ways to be charged with the crime of identity theft. If a person, without the victim's authorization, consent, or permission, and with intent to defraud for the person's own benefit or the benefit of a third party: (1) obtains, records, or accesses personal identifying information that would assist in accessing financial resources, obtaining identifying documents, or obtaining benefits from the victim; (2) obtains goods or services through the use of the victim's personal identifying information; or (3) obtains identifying document in the victim's name, the person commits identity theft.

[13] See, e.g., Appendix I and Appendix II (Delaware, Kansas, Missouri, New Jersey, New York, Pennsylvania, and Vermont).
[14] See, e.g., Appendix I and Appendix II (Alabama, Arkansas, Georgia, South Carolina, and Virginia).

Exceptions

Some states have created an exception to the crime of identity theft. Specifically, this crime is inapplicable to any person who obtains another's driver's license, or any other form of identification, for the sole purpose of misrepresenting age (e.g., to acquire alcohol, tobacco, or cigarettes, periodical, videotape, or other medium that contains nudity, or admittance to a live or film performance that prohibits minors).[15] Mississippi has noted that identity theft does not apply to persons who obtain or attempt to obtain personal identifying information of another pursuant to the discovery process of a civil action, administrative, or arbitration proceeding.

Enhanced Penalties

Lastly, some jurisdictions have awarded additional punishments to defendants convicted of identity theft. For example, a defendant may be ordered to pay restitution for the victim's financial loss, including correcting or clearing the victim's credit history, any civil or administrative proceeding costs to satisfy a debt, lien, judgment, or other obligation, lost wages, and reasonable attorney's fees.[16] In Massachusetts, Nevada, New Hampshire, New Mexico, and Washington, the defendant is court-mandated to pay these costs. Other examples include seizure and forfeiture of any property that is fraudulently obtained[17] and court authority to issue any order necessary to correct a public record that contains false information as a result of defendant's actions.[18]

Mail Theft

Hawaii Statutes

Mail theft is of considerable concern in the State of Hawaii. In the law enforcement community, mail theft is recognized as a predicate offense or precursor to identity theft. Last year, the U.S. Postal Inspection Service logged 7,404 mail theft complaints. In the first six months of this year, they recorded 4,260 complaints and it is estimated that there will be 10,000 mail theft complaints by the end of 2005. Notably, these numbers are representative of the people who report mail theft. They do not reflect a significant majority of people who do not report mail theft, generally because they are unaware that their mail had been stolen. Such record-setting activity has caused local law enforcement to double the number of postal inspectors and investigators chasing the thieves who steal mail in order to generate false identifications or conduct some type of fraudulent activity. Oftentimes drug users are used to steal mail in return for drugs or a percentage of the profit or return of the fraudulent activity so that they can purchase drugs. Presently, in accordance with state law, in cases where mail is stolen and a suspect is found in possession of other people's mail, the only state

[15] See, e.g., Appendix I (Alabama, Indiana, Kentucky, Louisiana, New Jersey, Oregon, Rhode Island, Vermont, Washington, and West Virginia).
[16] See, e.g., Appendix I and Appendix II (Illinois, Maryland, Missouri, Montana, Nevada, New Jersey, North Carolina, Texas, Virginia, Washington, and Wyoming).
[17] See, e.g., Appendix I and Appendix II (Iowa and Kentucky).
[18] See, e.g., Appendix I and Appendix II (Georgia, New Jersey, New Mexico, and Washington).

recourse available is to classify and charge such conduct as a misdemeanor or petty misdemeanor theft. This nominal criminal consequence is inadequate to address and deter and, in fact, it perpetuates the larger problem of identity theft.

Federal Statutes

In contrast, 18 U.S.C. § 1708 entitled "theft or receipt of stolen mail matter generally" provides:

> Whoever steals, takes, or abstracts, or by fraud or deception obtains, or attempts so to obtain, from or out of any mail, post office, or station thereof, letter box, mail receptacle, or any mail route or other authorized depository for mail matter, or from a letter or mail carrier, any letter, postal card, package, bag, or mail, or abstracts or removes from any such letter, package, bag, or mail, any article or thing contained therein, or secretes, embezzles, or destroys any such letter, postal card, package, bag, or mail, or any article or thing contained therein; or
>
> Whoever steals, takes, or abstracts, or by fraud or deception obtains any letter, postal card, package, bag, or mail, or any article or thing contained therein which has been left for collection upon or adjacent to a collection box or other authorized depository of mail matter; or
>
> Whoever buys, receives, or conceals, or unlawfully has in his possession, any letter, postal card, package, bag, or mail, or any article or thing contained therein, which has been so stolen, taken, embezzled, or abstracted, as herein described, knowing the same to have been stolen, taken, embezzled, or abstracted –
>
> Shall be fined under this title or imprisoned not more than five years, or both.

Federal sentencing for this crime is a fine up to $250,000, up to five years incarceration, and up to three years of supervised release following any period of incarceration. Additionally, as of July 2004, if a person commits this offense and then uses the mail obtained to commit crimes such as wire fraud, mail fraud, access device fraud, bank fraud, or computer fraud, 18 U.S.C. § 1208A enhances the punishment to a two-year mandatory sentence.

The State of Hawaii has no counterpart to this federal statute. As such, local law enforcement cannot properly or adequately address what has been seen as the precursor activity to identity theft.

Department of the Attorney General Hawaii High Technology Crime Unit Task Force Program

In May 2002, with funds from the Byrne Memorial State and Local Enforcement Assistance Formula Grant, the Department of the Attorney General established the

Hawaii High Technology Crime Unit (HHTCU) to increase the effectiveness and efficiency of investigations and prosecutions of computer related crimes in the State of Hawaii. The HHTCU accomplishes this goal by creating and administering a task force composed of federal, state, and county law enforcement agencies and by creating capabilities in investigations, forensics, prosecutions, and community outreach.

In recognition that identity theft, phishing, and other forms of electronic commerce-based crimes traverse jurisdictions and are often complicated by a multitude of transactions and a variety of victims, localized task forces are effective and necessary to coordinate investigations and share resources. The task force created by the HHTCU brings various law enforcement agencies together to collectively combat these crimes since the cost of creating a computer crime unit within each county police department would be prohibitive and not a fiscally sound use of the very limited law enforcement dollars.

The formation of a computer crime unit is not a new concept. Many state and local law enforcement agencies have developed computer crime units to combat the ever-increasing problem of cyber crime. Hawaii needs to have a properly trained and equipped computer crime unit to keep up with the high tech criminals and administer a task force to work collaboratively with other law enforcement agencies. The only way to protect our citizens is to ensure that local law enforcement has the ability to detect, investigate, and ultimately prosecute individuals who use their computers to carry out illegal activities, and to educate our public as to the nature of these crimes for proper prevention.

EDUCATIONAL AND OUTREACH INITIATIVES

Program Initiatives

Many states offer educational outreach programs through their respective Offices of the Attorney General or Offices of Consumer Protection. These programs include giving speeches and presentations to interested citizen groups, creating press releases, conducting training and continuing education classes for law enforcement officials, moderating Continuing Legal Education (CLE) courses for attorneys, and sending out guest columns about identity theft and related crimes. Following is a sampling of these initiatives:

- Alabama's education initiatives include a comprehensive information packet to be mailed to identity theft victims and a Consumer Protection Hotline available to all law enforcement entities that investigate and prosecute these offenses.
- Arkansas' Attorney General gives several speeches every week; nearly all deal with identity theft.
- The Florida Attorney General's office provides training sessions on identity theft and cyber crimes directed to law enforcement, prosecuting, and victim services audiences. The Attorney General's office also partners with the

Florida Crime Prevention Association to provide crime prevention training in Florida.[19]

- In Hawaii, the DCCA established an identity theft hotline (587-3222). Trained investigators are available to assist citizens via telephone with their inquiries.
- The Idaho Office of the Attorney General featured identity theft as its consumer protection theme at the county fairs in recent years.
- Oklahoma's Attorney General actively participates in educational programs in conjunction with the Federal Bureau of Investigation (FBI), the U.S. Postal Inspector, and others regarding identity theft and phishing throughout the state, including a special CLE class for attorneys who represent consumers. The office has also instigated a spam complaint process that is used to monitor phishing trends.
- Texas requires all commissioned peace officers to complete an identity theft training course developed by the Attorney General's office. Both the civil and criminal divisions of the Attorney General's office conduct outreach programs throughout the state.

PSAs and Community Service Programs

Another effective method of raising public awareness of identity theft and related crimes is via the print, radio, and television media. Public Service Announcements showcase common identity theft scenarios and demonstrate proper responses to the threats. The ads are aimed at vulnerable audiences and include contacts for additional information.

- The Alabama Attorney General's office created a series of public service announcements about identity theft that include contact information for the specially trained consumer specialists within the Attorney General's office working to protect victims' rights and restore their good names.
- The Florida Department of Highway Safety and Motor Vehicles generated a streaming video format public service announcement about identity theft available at www.hsmv.state.fl/IDtheft.html.
- Hawaii's Office of Consumer Protection and DCCA produced four public service announcements demonstrating common ways a person's identity can be stolen. The ads were funded by settlements of lawsuits brought by the Office of Consumer Protection on behalf of consumers.
- New Jersey radio stations aired public service announcements by the Attorney General warning residents about identity theft and common scams used to steal personal information.

[19] The Florida Crime Prevention website (www.floridacrimeprevention.org) describes itself as "a forum to exchange crime prevention ideas and educate Florida's citizens about methods of crime prevention".

Business Initiatives

Community initiatives are grassroots level efforts to educate consumers and businesses about electronic commerce-based crimes. Government, businesses, and non-profit organizations have developed programs to identify risky behavior and teach preventative or remedial measures.

The Hawaii Bankers Association, which includes American Savings Bank, Bank of Hawaii, HomeStreet Bank, Central Pacific Bank, First Hawaiian Bank, Bank of the Orient, Territorial Savings, and Hawaii National Bank, has disseminated educational information to its customers regarding the prevention of identity theft. This initiative includes branch handouts and a television, radio, and print campaign. Public Service Announcements emphasizing bank account security have been broadcast on local television stations. Messages are designed to alert vulnerable audiences of the dangers of identity theft and related crimes, and to demonstrate proper responses to common scenarios. Both the brochures and the Public Service Announcements include contacts for additional resources and information.

The Better Business Bureau office serving eastern Massachusetts, Maine, and Vermont launched a campaign in 2004 in partnership with local media and businesses about minimizing vulnerability to identity theft and related crimes. It also provided links to Better Business Bureau website banners for inclusion on a business or organization website to support identity theft awareness and to spread the word on preventing and addressing electronic commerce-based crimes.

Public-Private Partnership Initiatives

Federal agencies have formed public-private partnerships to provide resources for victims of cyber crime and for state and local law enforcement officials. Likewise, the states have joined together to share information in order to raise cyber security awareness nationwide and to improve Internet security and safety throughout the United States.

The Cyber Division of the FBI works to prevent criminals from using the Internet and online services to steal from, defraud, or otherwise victimize citizens, businesses, and communities. One of its missions is to form and maintain public-private alliances to maximize law enforcement response capabilities. Additional information about its operations and links to resources can be found at the Cyber Program Homepage (www.fbi.gov/cyberinvest/cyberhome.htm). Other federal public-private initiatives include the following:

- The Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center (NW3C). The IC3 provides a

central referral mechanism for law enforcement and regulatory agencies at the federal, state, and local levels.[20]

- The NW3C is a federally funded, non-profit corporation comprised of law enforcement agencies, state regulatory bodies with criminal investigative authority, and state and local prosecution offices. Its mission is to provide a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes and to support and partner with other appropriate entities in addressing homeland security initiatives, as they relate to economic and high-tech crimes.[21]
- The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. US-CERT was established in 2003 to protect the nation's Internet infrastructure.[22] US-CERT coordinates defenses against and responses to cyber attacks across the nation, and publishes current security alerts, current activities, and vulnerability resources, along with an array of publications and security documents on its website at www.uscert.gov.

The Multi-State Information Sharing Analysis Center (MS-ISAC) is a collaboration between forty-nine participating states, including Hawaii, and the District of Columbia.[23] The MS-ISAC was established in January 2003 to create a centrally coordinated mechanism for sharing important security intelligence and information among the states, thereby eliminating duplicative efforts by individual states. It also serves as a critical point of contact between the states and the federal government. The MS-ISAC member states meet monthly via teleconference to discuss issues and share information.

In conjunction with the U.S. Computer Emergency Response Team (US-CERT) and the National Cyber Security Alliance, the MS-ISAC celebrates the second annual National Cyber Security Awareness Month in October 2005. The MS-ISAC invited the nation's governors to sign a proclamation in recognition of Cyber Security Awareness Month and prepared resources designed to raise public awareness and preparedness, such as a cyber security toolkit distributed to the states.[24] The following items in the toolkit can be "branded" with business or school name and other relevant information:

- A cyber security awareness brochure

---

[20] For additional information about this program, see www.ic3.gov. Another cooperative venture between the FBI and the NW3C is the Internet Fraud Complaint Center (IFCC). Its mission is to combat fraud committed over the Internet and to provide a national consumer complaint mechanism. See www.ifccfbi.gov for details.

[21] Additional information about NW3C's actions and projects can be found at www.nw3c.org.

[22] US-CERT is the operational arm of the National Cyber Security Division of the Department of Homeland Security. See www.uscert.gov/aboutus.html for additional information.

[23] As of October 2005, Kansas is not a participating state.

[24] The Cyber Security Toolkit is available online at www.cscic.state.ny.us/msisac/ncsa/oct05/index.htm. Additional activities will be posted on this website throughout October 2005.

- Cyber security calendars designed especially for children, teens, and government/businesses and citizens
- Cyber security awareness posters appropriate for various audiences

SECTION 3

EXPLORE ANY OTHER OPTIONS AVAILABLE TO THE TASK FORCE TO DETER ELECTRONIC COMMERCE-BASED CRIMES FROM OCCURRING IN THE STATE.

Protection of Personal Identification Data

One area of particular concern to the Task Force is the number of Hawaii laws requiring individuals to provide nonpublic personal and financial information that subsequently becomes embedded in publicly accessible records. A preliminary scan of the Hawaii Revised Statutes (Appendix III) identified a range of Hawaii laws requiring this type of information. The best way to prevent exploitation of personal and financial information belonging to Hawaii residents is to provide greater protection for such information under Hawaii's public records and identity theft prevention laws.

Hawaii's public records law enumerates areas in which the individual has a significant privacy interest and authorizes disclosure of a government record only when the public interest in such disclosure outweighs the privacy interest of the individual.[25] Protected information includes an individual's financial information, social security number, and any information compiled in relation to an individual's fitness to be granted or to retain a license, with the exception of records of disciplinary action and complaints against a licensee, current employment information, and any required insurance coverage.

In 2005, Hawaii enacted two measures restricting the use of social security numbers on public records. Act 13 amends section 12-3, Hawaii Revised Statutes, to require only the last four digits of a voter's social security number on a candidate nomination paper. Act 85 amends section 92F-12, Hawaii Revised Statutes, to bar disclosure of the social security numbers of contract hires and consultants employed by state agencies.[26] Act 92, Session Laws of Hawaii 2004, exempts disclosure of social security numbers from government payroll records that are public information, restricts retail merchant card issuers from requesting personal information except for credit purposes, and prohibits the sharing of cardholder information.[27]

Briefly summarized below are categories of public records identified as potentially vulnerable to misuse.

Family Court Actions

Hawaii divorce, separation, and annulment proceedings are initiated by filing a complaint, summons, and Matrimonial Action Information form (MAI) with the Family Court.[28] The MAI requires the party initiating the proceedings to furnish,

[25] Section 92F-14, HRS.
[26] The text of these measures is available at www.capitol.hawaii.gov.
[27] For the text of this Act, see www.capitol.hawaii.gov.
[28] Section 580-1, HRS governs commencement of divorce, separation, and annulment actions in Hawaii. Although this section does not expressly require a Matrimonial Action Information form, the Family Court requires the Plaintiff to file one when initiating a divorce or separation action.

to the extent known, the social security number, business and residence telephone numbers, employer's name and address, and salary information for each party. Divorce judgments and paternity judgments also require inclusion of the parties' social security numbers.[29]

Family Court cases filed to establish or modify a support order or to determine parentage also require personal identifying information that becomes part of the court record. The petition or accompanying documents must state, so far as is known, the name, residential address, and social security numbers of the obligor and the obligee, and the name, sex, residential address, social security number, and date of birth of each child for whom support is sought.[30]

Judgments

All judgments affecting the title to real property must include the social security number, general excise tax number, or federal identification number for persons, corporations, partnerships, or other entities against which the judgment is rendered.[31] Except as otherwise provided, every judgment shall contain or have endorsed on it the social security number, State of Hawaii general excise taxpayer identification number, or federal employer identification number for persons, corporations, partnerships, or other entities against whom the judgment is rendered.[32] This includes every judgment recorded by the Bureau of Conveyances[33] and judgments of federal courts recorded in either the Bureau of Conveyances or Land Court.[34]

Other Approaches

Submitting separate confidential information forms and sealed financial source document forms. Minnesota law requires the provision of social security numbers for parties to divorce or separation actions involving child or spousal support.[35] In addition, the parties are required to serve and file documentation of earnings and income.[36] Under this chapter, social security numbers and tax returns are not accessible to the public. To ensure the confidentiality of social security numbers and financial documents, court rules require their submission on separate sheets entitled "Confidential Information Form" and "Sealed Financial Source Documents" respectively.[37]

Designating a date after which social security numbers are excluded. Florida's public records law designates a date after which social security numbers may not

[29] Section 571-84.5 (divorce) and sections 584-3.5 and 584-23.5 (paternity), HRS.
[30] Section 576B-311, HRS.
[31] Section 501-151, HRS.
[32] Section 636-3, HRS.
[33] Section 502-033, HRS.
[34] Section 504-1, HRS.
[35] Section 518.10, Minnesota Revised Statutes (2004).
[36] Section 518.551 Subd. 5b, Minnesota Revised Statutes (2004).
[37] Minn. Gen. R. Prac. 11.

be included in documents recorded with the county recorder.[38] Social security numbers included in documents filed prior to that date may be made available as part of the official record available for public inspection and copying. However, the statute further provides that any person, or his or her attorney or legal guardian, may request that the county recorder remove the social security number from an official record made electronically available to the general public.

Authorize security alerts and security freezes for consumer credit reports. Texas and Louisiana consumers have the option to place an alert about possible unauthorized credit activities on credit records and/or a freeze to prevent unauthorized release of credit information.[39]

Verification of social security number by Notary Public. California recently enacted legislation eliminating social security numbers from statutory power of attorney forms. Instead, a notary public would record the last four digits of a person's social security number after verifying identity via an acceptable form of identification.[40]

Issue identity theft passport. Several states passed a measure authorizing the issuance of identity theft passports to identity theft victims.[41]

[38] Sections 119.071(5)(a)7.a to 119.071(5)(a)7.c, 2005 Florida Statutes.
[39] Two examples of security alert and freeze statutes are: Texas Statutes chapter 20 and Louisiana Revised Statutes sections 3571.1 et seq.
[40] S.B. No. 158 was signed by the California governor on September 22, 2005.
[41] Act 744 was signed by the Arkansas governor on March 10, 2005; H.B. 110 was signed by the Montana governor on March 24, 2005; S.B. No. 304 was signed by the Nevada governor on June 8, 2005.

SECTION 4

ESTABLISH FINDINGS AND DEVELOP RECOMMENDATIONS ON HOW THE STATE MAY BEST DETER ELECTRONIC COMMERCE-BASED CRIMES FROM OCCURRING IN THE STATE.

Findings and Recommendations

(1) Due to the lack of financial resources and training, the law enforcement community has banded together to form working groups to more efficiently and effectively address the issue of identity theft in Hawaii. Without a strong working relationship between federal, state, and county law enforcement, the crime of identity theft cannot and will not be adequately addressed. The Task Force supports an expanded law enforcement effort between the U.S. Attorney, the Attorney General, county police departments, and related federal agencies.

- Specific Action: Ensure the Department of the Attorney General Hawaii High Technology Crime Unit (HHTCU) is fully funded whether through grants or state funds. When properly funded, the HHTCU should be responsible for creating a law enforcement task force to coordinate enforcement efforts between federal, state, and county law enforcement and to provide training in the area of detection, investigation, and prosecution of identity theft. The law enforcement task force should also support increased community outreach and educational partnerships among business, community, and governmental agencies.

(2) Law enforcement agencies in Hawaii have found it difficult to curb the rise in identity theft related crimes because identity thieves in possession of personal information that have not yet caused a monetary loss to the victim cannot be prosecuted for crimes other than petty misdemeanors. The Task Force supports legislation that will provide law enforcement with more efficient enforcement and stricter enforcement penalties for identity theft crimes.

- Specific Action: Amend Hawaii Revised Statutes section 708-839.8, Identity Theft in the Third Degree to include a crime for possession or transfer of "confidential personal information" and Hawaii Revised Statutes section 706-606.5 to include Identity Theft as a repeatable offense. A draft of the proposed legislation is in Appendix IV.

(3) Hawaii's drug epidemic has been viewed by law enforcement as a major cause of identity theft related crimes in Hawaii. Understanding the relationship between those that illegally use drugs and identity theft will aid law enforcement and the public in better understanding how to address the growing problem of identity theft. The Task Force supports law enforcement in determining whether there is a nexus between illegal drug use and identity theft to allow for a more efficient and effective response to identity theft.

- Specific Action: Provide funding to the Department of the Attorney General, Crime Prevention Justice Assistance Division to conduct a study as to what effect drug use has upon the crime of identity theft.

(4) Law enforcement agencies in Hawaii track identity theft crimes in a variety of ways. The current tracking mechanism does not promote accurate and useful statistical information. In order to create a superior understanding of the depth and pervasiveness of the identity theft problem in Hawaii the Task Force supports a uniform reporting system for identity theft crimes.

- Specific Action: Provide funding to the Department of the Attorney General, Crime Prevention Justice Assistance Division to determine a common definition for identity theft and develop a uniform reporting system to facilitate the reporting and tracking of identity theft crimes in Hawaii.

(5) Identity theft cannot be committed unless personal information about a particular person can be obtained. The Task Force has identified numerous state agencies that routinely collect and store personal information of State residents. Personal information is easily obtainable through public records checks or formal public records requests. The Task Force supports legislation that will more effectively protect personal information that is currently available to the general public.

- Specific Action: Amend various Hawaii Revised Statues relating to court records and other public records that include personal information such as social security numbers.

(6) The problem of identity theft will continue to rise unless government, law enforcement and the general public begin to better protect their personal information. The Task Force supports the continuation of the Hawaii Anti-phishing Task Force in order to continue the development of state initiatives on how best to prevent identity theft crimes in the State.

- Specific Action: Rename the Hawaii Anti-phishing Task Force to the Hawaii Identity Theft Task Force. Create the Hawaii Identity Theft Task Force as a legislative task force. The Hawaii Identity Theft Task Force should include the current members of the Hawaii Anti-phishing Task Force with the addition of a member from the Hawaii Prosecuting Attorneys' Association; a member from the Administrative Director of the Courts or the Administrative Director's designee; and a member from the Honolulu field office of the United State Postal Inspection Service. A draft of the proposed legislation is in Appendix IV.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
Alabama	§§ 13A-8-190 to 13A-8-201	The Consumer Identity Protection Act defines identity theft and related offenses. Classifies offenses based on financial loss. Creates an inference of intent to manufacture, sell, transfer, or purchase identification documents or identifying information for the purpose of committing identity theft based on trafficking in stolen identities or unauthorized possession of five or more identification documents of the same person, or of five or more separate persons. Trafficking in stolen identities is a Class B felony. Governs obstructing justice using a false identity. Allows restitution for financial loss. Authorizes court to annotate court records to reflect innocence of victim or to issue an order to correct records. Creates a civil cause of action for identity theft victims. Allows adding a block on false information in credit reports, and reissue of identification documents for identity theft victims.
Alaska	§ 11.46.180	Defines theft by deception as when, with intent to deprive another of property or to appropriate property of another to oneself or a third person, a person obtains the property of another by deception. Lists classification of offenses.
	§ 11.46.290	Makes obtaining an access device or identification document by fraudulent means a Class A misdemeanor.
	§ 11.46.565	Prohibits the unauthorized possession or use of an access device or identification document of another person to obtain a false identification document, open an account at a financial institution, to obtain an access device, or to obtain property or services that recklessly damage the financial reputation of the other person. Criminal impersonation in the first degree is a class B felony.
	§ 28.10.505	Limits disclosure of personal information contained in motor vehicle records.
Arizona	§§ 13-2008	Defines taking identity of another person or entity as the use of identifying information without consent, with the intent to obtain or use the identity for any unlawful purpose or to cause loss, whether or not the person or entity actually suffers any economic loss as a result of the offense. Taking the identity of another person or entity is a Class 4 felony.
	§ 13-2009	Defines the aggravated taking identity of another person or entity as involving five or more victims or when actual economic loss totals $3,000 or more. Aggravated taking identity of another person or entity is a Class 3 felony.
	§ 13-2010	Prohibits trafficking in the identity of another person or entity, which is knowingly selling, transferring or transmitting identifying information of another person or entity, without consent, for any unlawful purpose or to cause loss to the person or entity, whether or not the other person or entity actually suffers any economic loss. Trafficking in the identity of another person or entity is a Class 2 felony.
Arkansas	§ 5-37-227	Defines financial identity fraud as when a person appropriates, accesses, obtains, records, or submits to a financial institution another person's identifying information for the purpose of opening or creating a credit account, debit account, or financial resource without the authorization of the person identified by the information. Financial identity fraud is a Class C felony.
	§ 5-37-228	Creates an identity theft passport program. Authorizes the Attorney General, in cooperation with any law enforcement agency, to issue an identity theft passport to a state resident who learns or reasonably suspects that he or she is the victim of financial identity fraud.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES ENACTED PRIOR TO 2005

State	Statute	Summary
California	Civil Code § 1785.11.1	Authorizes security alerts in credit reports at the request of consumers. "Security alert" means a notice placed in a consumer's credit report that notifies a recipient of the credit report that the consumer's identity may have been used without consent to fraudulently obtain goods or services in the consumer's name.
	Civil Code § 1785.11.2	Authorizes security freezes on credit reports upon written request of consumers. "Security freeze" means a notice placed in a consumer's credit report that prohibits the consumer credit reporting agency from releasing the credit report or any information from it without the express authorization of the consumer.
	Civil Code § 1798.85	Regulates usage of social security numbers in public display and for identification purposes.
	Penal Code § 530.6	Authorizes a person who learns or reasonably suspects that he or she is the victim of identity theft to file a police report. Identity theft victims whose information has been used unlawfully by another may petition the court for an expedited factual determination of innocence.
	Penal Code § 530.7	Directs the California Department of Justice to establish and maintain a database of individuals who have been victims of identity theft. Limits access to the database to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.
	Penal Code § 530.8	Governs the disclosure to identity theft victims of information provided on fraudulent applications in their names.
	Penal Code § 964	Provides protection for confidential personal information in police reports.
	Penal Code §§ 530 to 530.5	Prohibits intentional false impersonation of another to obtain money or property. Includes penalties in the same manner and to the same extent as for larceny of the money or property so received. Prohibits willfully obtaining the personal identifying information of another person and using it for any unlawful purpose without the consent of that person.
Colorado	§ 10-3-129	Prohibits the inclusion of social security numbers on insurance identification cards or proof of insurance cards after January 1, 2006. Requires an insurance company or insurer to reissue to the insured an insurance identification card or proof of insurance card that does not display the insured's social security number upon request by the insured prior to January 1, 2006.
	§ 10-4-16	Prohibits using independently corroborated identity theft as a negative factor in an insurance scoring methodology or in reviewing credit information for the purpose of underwriting or rating a policy of personal lines of property and casualty insurance.
	§ 13-21-109.5	Prohibits fraudulent use of social security numbers and provides for recovery of damages caused thereby.
	§ 13-21-122	Creates a civil right of action against the perpetrator who committed a crime using personal identifying information of another in the commission of a crime, regardless of whether the perpetrator was convicted of the crime. Authorizes recovery of actual damages, including, but not limited to, costs associated with repairing damage to reputation or credit rating, attorney's fees and costs, and punitive damages.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
	§ 16-5-103	Allows the court to make a factual determination of innocence of an identity theft victim and to order annotation of court records and documents to show that the information is not accurate and does not reflect the perpetrator's identity. Applies to a person whose identifying information has been mistakenly associated with an arrest, summons, indictment, or conviction.
	§ 18-5-113	Defines criminal impersonation as knowingly assuming a false or fictitious identity or capacity, and acting in a way that might subject the falsely impersonated person to civil or criminal action or acting with intent to unlawfully gain a benefit for himself or another or to injure or defraud another. Criminal impersonation is a Class 6 felony.
	§ 18-5-117	Prohibits unlawful possession of personal identifying information of another person with the intent to use the information, or to aid or permit another to use the information, to unlawfully gain a benefit for himself or herself or another person, or to injure or defraud another person. Unlawful possession of personal identifying information is a Class 1 misdemeanor.
	§ 18-5.5-102	Outlaws accessing any computer, computer network, or computer system for the purpose of devising, or executing any scheme or artifice to defraud or to commit theft. Classification of violations is based upon damages and prior violations.
	§ 24-33-110	Requires applications for licenses issued by the Colorado Department of Natural Resources (DNR) to include the applicant's name, address, and social security number; except that the Division of Wildlife shall not collect applicants' social security numbers on license applications unless required by federal law or mandated as a condition receiving federal funds. Prohibits inclusion of social security numbers on licenses issued by the DNR.
	§ 24-72.3-102	Limits a public entity's inclusion of social security numbers on licenses, permits, passes, or certificates. Prohibits a public entity from requesting a person's social security number over the phone, the Internet, or via mail. Lists exceptions to this prohibition.
	§ 42-1-222	Directs the Colorado Department of Motor Vehicles to create a motor vehicle investigations unit to investigate and prevent fraud involving the use of driver's licenses, identification cards, and other motor vehicle documents issued by the department. Instructs the unit to assist victims of identity theft involving such documents.
	§ 42-2-118 (1.5)(f)	Requires the Colorado Department of Motor Vehicles to identify risks and designate measures the department will implement to minimize opportunities for identity theft and fraud.
	§ 5-3.7-101	Requires verification of a consumer's address when an acceptance of a firm offer of credit lists the address of the consumer accepting the offer as different from the address to which the offer was sent. Requires the solicitor to verify that the consumer accepting the offer is the same consumer to whom the offer was sent before issuing or directing issuance of credit.
	§§ 7-90-306(5) to 7-90-306(6)	Authorizes the Colorado secretary of state to remove personal identifying information from the publicly accessible documents and other records maintained by that office, if the information is not required by law to be included in the documents and records. Defines "personal identifying information."

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES ENACTED PRIOR TO 2005

State	Statute	Summary
Connecticut	§ 53a-129a	Defines identity theft as when a person intentionally obtains personal identifying information of another person without authorization and uses that information to obtain or attempt to obtain, money, credit, goods, services, property, or medical information in the name of such other person. Defines "personal identifying information."
	§§ 53a-129b to 53a-129d	Classifies identity theft in the first, second, and third degrees.
	§ 53a-129e	Defines trafficking in personal identifying information as when an unauthorized person sells, gives, or otherwise transfers the personal identifying information of another person to a third person, knowing that such information has been obtained without the authorization of such other person, and that the third person intends to use the information for an unlawful purpose. Trafficking in personal identifying information is a Class D felony.
	§ 54-1n	Outlines the responsibilities of law enforcement in cases of identity theft.
	§ 54-93a	Authorizes the court to issue an order to correct a public record that contains false information as a result of identity theft.
Delaware	Title 11 §854	Defines identity theft as when a person knowingly or recklessly obtains, produces, possesses, uses, sells, gives, or transfers personal identifying information belonging or pertaining to another person without consent and with intent to use the information to commit or facilitate a crime. Defines "personal identifying information." Identity theft is a Class D felony.
District of Columbia	§§ 22-3227.01 to 3227.08	Defines identity theft, establishes jurisdiction, enumerates penalties, including restitution and enhanced penalties for committing the offense of identity theft against an individual who is 65 years of age or older at the time of the offense. Requires police to make a report of each complaint of identity theft. Authorizes the court to issue an order to correct a record that contains false information due to identity theft.
Florida	§§ 817.568 to 817.569	Defines fraudulent use of personal identification information, criminal use of a public record, and related crimes and terms, enumerates penalties and sentencing guidelines. Authorizes a prosecutor to move for a suspended sentence for a convicted individual who provides substantial assistance in the identification, arrest, or conviction of accomplices, accessories, co-conspirators, or others involved in perpetrating these crimes.
Georgia	§ 16-9-121	Defines financial identity fraud as the unauthorized use of another person's personal information with the intent to unlawfully appropriate resources and obtain or record identifying information of a person that would assist in accessing the resources of that person or any other person, or to access or attempt to access the resources of a person through the use of identifying information.
	§§ 16-9-123 to 16-9-128	Authorizes the investigation of claims of identity fraud. Requires transmission of copies of all reports to the Georgia Governor's Office of Consumer Affairs. Information in the repository is available for law enforcement agencies, but is not available to the public. Authorizes the Attorney General and prosecutors to conduct criminal prosecution of all cases of identity fraud. Establishes jurisdiction, enumerates penalties, and lists exceptions for the use of personal identifying information.
Hawaii	§§ 708.839.6 to 708-839.8	Defines identity theft as when a person makes or causes to be made, either directly or indirectly, a transmission of personal information of another with the

State	Statute	Summary
		intent to commit unlawful acts. Classification of offenses is based on underlying unlawful acts.
Idaho	§ 18-3126	Prohibits obtaining or recording personal identifying information of another person without authorization, with the intent that the information be used to obtain, or attempt to obtain, credit, money, goods, or services in the name of the other person. Classification of offenses is based on retail value of fraudulently obtained items.
	§ 18-3127	Outlaws receiving or possessing fraudulently obtained goods or services. Prohibits a person who knows, or has reason to believe, it has been obtained by fraud from receiving, retaining, concealing, possessing, or disposing of personal property, cash, or other thing of value.
	§ 18-3128	Provides penalties for violations of previous sections. Classification of offenses is predicated on amount of loss.
	§ 49-203	Prohibits the knowing disclosure of personal identifying information contained in a motor vehicle or driver record, except in certain circumstances.
Illinois	720 ILCS § 5/16G-20	Prohibits aggravated identity theft, which involves identity theft against a victim who is 60 years of age or older or a disabled person. Classification of offenses is based on monetary value of loss.
	720 ILCS §§ 5/16G-1 to 5/16G-19	Identity Theft Law. Describes legislative intent. Defines identity theft, "personal identifying information," and other terms. Discusses public policy associated with identity theft. Prohibits transmission of personal identifying information. Classification of offenses is based upon monetary value of loss.
	720 ILCS 5/16G-21	Creates a civil cause of action by identity theft victims. Allows an identity theft victim who suffered damages as a result of the violation to recover court costs, attorney's fees, lost wages, and actual damages.
	720 ILCS 5/16G-30	Mandates law enforcement agencies to accept identity theft reports. Authorizes the judge to make a factual determination of innocence for actual or suspected identity theft victims and to seal, delete, or label public records to identify data as impersonated and not reflective of the identity theft victim.
Indiana	§ 34-43-5-3.5	Prohibits identity deception, which is knowingly or intentionally obtaining, possessing, transferring, or using the identifying information of another person without authorization, to harm or defraud another person, assume another person's identity, or profess to be another person. Enumerates exceptions. Identity deception is a Class D felony.
	§ 35-43-5-1	Contains definitions of terms, including "identifying information."
	§ 9-14-3.5	Governs disclosure of personal information and social security numbers contained in motor vehicle records. Prohibits release of personal identifying information except in certain circumstances. Defines "personal identifying information" and other terms.
	§ 9-14-3.5-10	Authorizes limited disclosure by the Indiana Bureau of Motor Vehicles of personal information from motor vehicle records.
	§ 9-14-3.5-10.5	Prohibits disclosure by the Indiana Bureau of Motor Vehicles of personal identifying information contained it its files, except in limited circumstances.
	§ 9-14-3.5-12	Authorizes the Indiana Bureau of Motor Vehicles to require any person requesting information to satisfy certain conditions before releasing personal identifying information to that person.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
	§ 9-14-3.5-15	Prohibits requesting the disclosure of personal information from the Indiana Bureau of Motor Vehicle records by knowingly or intentionally misrepresenting a person's identity or making a false statement to the bureau on an application. Misrepresenting information on an application is a Class C misdemeanor.
Iowa	§ 714.16B	Authorizes a civil cause of action, in addition to any other remedies provided by law, for a person suffering pecuniary loss as a result of an identity theft. Calculates damages as $1,000 or three times the actual damages, whichever is greater, along with reasonable attorney's fees and court costs.
	§ 715A.8	Defines identity theft as when a person fraudulently uses or attempts to fraudulently use identification information of another person, with the intent to obtain credit, property, services, or another benefit. Describes "identifying information." Classification of offenses is based on amount of financial loss.
	§ 715A.9	Clarifies the method for calculating financial loss by identity theft victims.
Kansas	§ 21-4018	Defines identity theft as knowingly, and with intent to defraud for economic benefit, obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, identification documents or personal identification number of another person. Classifies offense as a severity level 7 person felony.
Kentucky	§ 514.160	Defines theft of identity as unauthorized use of the personal data of another person, with the intent to represent that he or she is the other person to deprive that person of property, obtain benefits or property to which he or she would otherwise not be entitled, avoid detection, or for political or commercial benefit. Describes "identifying information." Establishes venue. Theft of identity is a Class D felony.
	§ 514.170	Outlaws trafficking in stolen identities, which is when a person manufactures, sells, transfers, or purchases, or possesses with the intent to manufacture, sell, transfer, or purchase, the personal identity of another person for an unlawful purpose.
Louisiana	RS § 14:67.16	Defines identity theft as the unauthorized use, or attempted use with fraudulent intent, of personal identifying information of another person to obtain, whether contemporaneously or not, credit, money, goods, services, or anything else of value. Enables a victim to initiate a law enforcement investigation. Classification of offenses is based on value of property, benefits, or anything else of value acquired by the perpetrator. Requires defendant to pay restitution, and empowers the court to establish a payment plan if there is no money available to the defendant.
Maine	Title 17-A § 905-A	Defines misuse of identification as when, in order to obtain confidential information, property or services, a person intentionally or knowingly presents or uses an account, credit or debit card, or form of identification that is stolen, forged, canceled or obtained as a result of fraud or deception, or which the person is otherwise not authorized to use. Misuse of identification is a Class D crime.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
Maryland	§8-301	Prohibits identity fraud, which is the unauthorized use of the identity of another to avoid identification, apprehension, or prosecution for a crime, or knowingly possessing or obtaining the personal identifying information of another in order to use, sell, or transfer the information to get a benefit, credit, goods, services, or other thing of value. Establishes venue and creates statewide jurisdiction for state police, and other law enforcement officers, and details associated rights and responsibilities. Authorizes restitution to the victim for reasonable costs associated with clearing the victim's name or good credit, or debt collection proceedings, including attorney's fees. Enumerates penalties and statute of limitations. Authorizes the State's Attorney or Attorney General to investigate and prosecute identity theft crimes.
	§8-304	Enables a person who knows or reasonably suspects that he or she is the victim of identity theft to make a report to a local law enforcement agency. Authorizes the local agency to subsequently refer the matter to the law enforcement agency with proper jurisdiction.
Massachusetts	Ch. 266 § 37E	Defines the use of personal identification of another, identity fraud, and related terms. Provides penalties and authorizes restitution for financial losses suffered by a victim as the result of the violation, including costs associated with clearing the victim's name or good credit, debt collection proceedings, lost wages, and attorney's fees.
Michigan	§§ 445.65 to 445.77	Identity Theft Protection Act. Specifies prohibited acts and practices concerning identity theft. Enumerates the powers and duties of state and local governmental officers and entities. Prescribes penalties and provides remedies. Establishes affirmative defenses.
	§ 445.83	Social Security Number Privacy Act. Describes prohibited uses and displays of social security numbers. Prescribes penalties and provides remedies.
Minnesota	§ 609.527	Defines identity theft as the transfer, possession, or use of an identity that is not a person's own, with the intent to commit, aid, or abet any unlawful activity. Defines related terms. Provides penalties and directs the court to order restitution to identity theft victims.
Mississippi	§ 97-19-11	Outlaws making a false statement in writing in order to procure the issuance of a credit card. Making a false statement in writing to obtain a credit card is a misdemeanor.
	§ 97-19-83	Prohibits the fraudulent use of mail or other means of communication to defraud, or to obtain money, property or services, or to unlawfully avoid the payment or loss of money, property or services, or for securing business or personal advantage by false or fraudulent pretenses. Establishes venue.
	§ 97-19-85	Outlaws the fraudulent use of identity, social security numbers, credit or debit card numbers, or other identifying information to obtain anything of value. Provides penalties. Authorizes restitution for identity theft victims.
	§§ 97-45-1 to 97-45-31	Computer Crimes and Identity Theft. Provides definitions of identity theft and other prohibited behavior. Authorizes the Attorney General of Minnesota to investigate identity theft and computer crimes, to issue subpoenas, and to distribute identity theft passports for identity theft victims. Allows victims to expunge records of false charges accrued on account of the activities of the perpetrator.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES ENACTED PRIOR TO 2005

State	Statute	Summary
	§ 97-9-79	Prohibits making or causing to be made any false statement or representation as to a person's identity, social security number, or other identifying information with the intent to mislead to a law enforcement officer in the course of the officer's duties. False statement of identity is misdemeanor.
Missouri	§ 570-224	Prohibits trafficking in stolen identities, which is when a person manufactures, sells, transfers, purchases, or possesses, with intent to sell or transfer, identification for the purpose of committing identity theft.
	§ 570.223	Defines identity theft as knowingly and with the intent to deceive or defraud obtaining, possessing, transferring, using, or attempting to obtain, transfer or use one or more means of identification not lawfully issued for his or her use. Authorizes the court to order restitution to an identity theft victim for any costs incurred by the victim, including attorney's fees.
Montana	§ 45-6-332	Defines theft of identity as when a person purposely or knowingly obtains personal identifying information of another person and uses that information for any unlawful purpose, including to obtain or attempt to obtain credit, goods, services, financial information, or medical information in the name of the other person without the consent of the other person. Defines "personal identifying information." Classification of offenses is based upon amount of economic benefit or loss.
Nebraska	§ 28-608	Prohibits criminal impersonation, which includes accessing or attempting to access the financial resources of another through the use of a personal identification document or personal identifying information for the purpose of obtaining credit, money, goods, services, or any other thing of value. Classification of offenses is based on the value that was gained or was attempted to be gained and subsequent offenses.
	§ 28-620	Outlaws the unauthorized use of a financial transaction device, which includes purposely or knowingly obtaining personal identifying information of another person and using that information for any unlawful purpose, including to obtain or attempt to obtain credit, goods, services, financial information, or medical information in the name of the other person without the consent of the other person.
Nevada	§§ 205.461 to 205.4657	Governs unlawful acts regarding personal identifying information. Prohibits obtaining and using personal identifying information of another person to harm the person or for unlawful purposes. Forbids the possession or sale of personal identifying information to establish false status or identity. Requires prosecution of offense regardless of whether the victim is living or dead. Authorizes the Attorney General of Nevada to create a program of restitution for identity theft victims.
New Hampshire	§ 638:26	Prohibits posing as another person to obtain money, credit, goods, services, or anything else of value or the unauthorized obtaining or recording personal identifying information about another person with the intent to pose as such person. Requires restitution for economic loss sustained by a victim as a result of such violation. Identity fraud is a Class A felony.
New Jersey	§ 2C:21-17	Defines offenses of impersonation and false identity. Classification of offenses is based on the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the injury or fraud perpetrated on another.
	§ 2C:21-17.1	Provides restitution for victims of personal identification information offenses.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
	§ 2C:21-17.3	Prohibits trafficking in personal identifying information, which is knowingly distributing, manufacturing or possessing personal identifying information of another person without authorization and with knowledge that the actor is facilitating a fraud or injury. Trafficking in personal identifying information is a crime of the fourth degree. Provides enhanced penalties for offenses involving 20 or more items of personal identifying information.
	§ 2C:21-17.4	Creates civil cause of action for damages resulting from use of personal identification information. Authorizes recovery of losses resulting from the use of a person's identifying information.
	§ 2C:21-17.5	Authorizes the court to order all consumer reporting agencies doing business within the State of New Jersey to delete items of information in a victim's file resulting from the unlawful use of the victim's personal identifying information. Requires the consumer reporting agency to provide the victim with a complimentary copy of any corrected credit report.
	§ 2C:21-17.6	Directs local law enforcement officials to take a report from a person who is or reasonably believes he or she is the victim of identity theft, regardless of whether jurisdiction lies elsewhere. Allows local officials to subsequently refer the complaint to a law enforcement agency in the proper jurisdiction.
New Mexico	§ 30-16-24.1	Defines theft of identity as willfully obtaining, recording, or transferring personal identifying information of another person without authorization, and with the intent to defraud that person or another. Describes obtaining identity by electronic fraud as knowingly and willfully soliciting, requesting, or taking any action by means of a fraudulent electronic communication with intent to obtain the personal identifying information of another. Directs the sentencing judge to issue written findings of fact and authorizes the court to issue orders to correct a public record that contains false information as a result of the theft of identity or of obtaining identity by electronic fraud.
New York	Penal Code § 190.77	Defines terms related to identity theft.
	Penal Code § 190.84	Establishes as an affirmative defense that the use of the personal identifying information of another was to misrepresent age in order to gain access to age-restricted premises, or to purchase alcohol or tobacco products.
	Penal Code §§ 190.78 to 190.80	Describes identity theft as when a person knowingly and with intent to defraud assumes the identity of another person. Classification of offenses is based on related offenses, the aggregate value of fraudulently obtained goods, and on prior identity theft convictions.
	Penal Code §§ 190.80 to 190.83	Defines unlawful possession of personal identifying information as when a person knowingly possesses another person's personal identifying or financial information, knowing that such information is intended to be used in furtherance of the commission of a crime. Classification of offenses is based on the quantities of personal identifying information in the possession of the perpetrator, having and supervising accomplices, and prior convictions.
North Carolina	§ 1-539.2C	Authorizes civil cause of action for identity theft victims. Provides damages of up to $5,000 for each incident or three times actual damages, whichever is greater, and attorney's fees. Establishes venue for civil actions and clarifies that civil action is not dependent on whether criminal prosecution has been or will be instituted against the perpetrator.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
	§ 14-113.20	Defines financial identity fraud as when a person knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to make financial or credit transactions in the other person's name, to obtain anything of value, benefit, or advantage, or for the purpose of avoiding legal consequences. Defines personal identifying information. Clarifies exceptions.
	§ 14-113.20A	Creates the offense of trafficking in stolen identities, which is when a person sells, transfers, or purchases the identifying information of another person with the intent to commit financial identity fraud, or to assist another person in committing financial identity fraud. Trafficking in stolen identities is a felony.
	§ 14-113.21	Establishes venue for criminal prosecution of financial identity fraud as any county in which any part of the financial identity fraud occurred, regardless of whether the defendant was ever actually present in that county.
	§ 14-113.22	Provides that financial identity fraud is a felony. Includes enhanced penalties when a victim suffers arrest, conviction, or detention as a proximate result of the fraud. Authorizes the court to order restitution for financial losses, including costs associated with repairing a victim's credit. Directs inclusion of notice in court records that the person whose identity was falsely used to commit the crime did not commit the crime.
	§ 14-113.23	Grants authority to the Attorney General of North Carolina to investigate complaints regarding financial identity fraud. Directs the Attorney General to refer all cases of financial identity fraud to the district attorney in the county where the crime was committed.
North Dakota	§ 12.1-23-11	Prohibits the unauthorized use or attempted use of the personal identifying information of another to obtain anything of value. Defines "personal identifying information." Classification of offenses is based on amount of damages. Provides enhanced penalties for subsequent violations, which may include a plea or conviction of guilt for violations of equivalent state or federal laws.
Ohio	§ 2913.49	Outlaws creating, using, obtaining, or holding out the personal identifying information of another as a person's identifying information. Also prohibits a person from authorizing, with intent to defraud, another person to use his or her personal identifying information. Classification of offenses is based on the value of the credit, property, services, debt, or other legal obligation involved in the violation or course of conduct. Establishes affirmative defenses.
Oklahoma	21§1533.1	Defines identity theft as willfully, and with fraudulent intent, obtaining the personal identifying information of another person, living or dead, with the intent to use or sell such personal identifying information to attempt to obtain credit, goods, property, or service in the name of the other person without the consent of that person. Prohibits creating or altering personal identifying information for fraudulent purposes. Authorizes the victim of identity theft to bring a civil action for damages against any person participating in furthering the crime or attempted crime of identity theft. Classifies identity theft as a felony.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
Oregon	§ 165.800	Defines identity theft as when a person, with the intent to deceive or to defraud, obtains, possesses, transfers, creates, utters or converts to the person's own use the personal identification of another person. Defines "personal identifying information." Establishes as an affirmative defense that the use of the personal identifying information of another to misrepresent age in order to gain access to age-restricted premises or benefits, or to purchase alcohol or tobacco products. Identity theft is a Class C felony.
	§ 314.840	Governs release of taxpayer information by the Oregon Department of Revenue.
Pennsylvania	18 Pa.C.S.A. § 4120	Defines identity theft as possessing or using identifying information of another person without consent to further any unlawful purpose. Authorizes the Attorney General of Pennsylvania to investigate and to institute criminal proceedings for identity theft violations any series of such violations involving more than one county of the commonwealth or another state. Defines "identifying information." Classification of offenses is based on total value involved. Provides enhanced penalties for third or subsequent offense or when a victim is 60 years of age or older.
Rhode Island	Chapter 11-49.1	Impersonation and Identity Fraud Act. Defines identity theft and related terms. Prohibits production, use, transfer, or possession of false identity documents. Exempts from prosecution for identity theft people under twenty-one years of age who use false identity documents for purposes of obtaining alcoholic beverages. Provides enhanced penalties for subsequent offenses. Authorizes search warrants and forfeiture of goods; describes use of proceeds from sale of forfeited goods.
South Carolina	§§ 16-13-500 to 16-13-530	Personal Financial Security Act. Defines "financial identity fraud" and "personal identifying information." Authorizes the court to order restitution to victim. Establishes venue as any county in which any part of the financial identity fraud occurred, regardless of whether the defendant was ever actually present in that county. Lists exemptions to the Act. Financial identity fraud is a felony.
South Dakota	§ 22-30A-3.1	Defines misdemeanor identity theft as when a person, without the authorization or permission of another person, and with the intent to deceive or defraud, obtains, possesses, transfers, uses, attempts to obtain, or records identifying information not lawfully issued for that person's use, or accesses or attempts to access the financial resources of that person through the use of identifying information. Effective July 1, 2006 § 22-40-8 will replace § 22-30A-3.1, making identity theft a felony.
	§§ 22-30A-3.2 to § 22-30A-3.3	Defines "identifying information." Establishes venue as any county in which any part of the financial identity fraud occurred, regardless of whether the defendant was ever actually present in that county. Effective July 1, 2006, §§ 22-40-9 to 22-40-10 will replace §§ 22-30A-3.2 to 22-30A-3.2.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
Tennessee	§ 39-14-150	Identity Theft Victims Rights Act. Defines identity theft as when a person knowingly obtains, possesses, buys, or uses the personal identifying information of another with the intent to commit any unlawful act without consent or lawful authority. Defines identity theft trafficking as when a person knowingly sells, transfers, gives, trades, loans or delivers, or possesses with the intent to sell, transfer, give, trade, loan or deliver the personal identifying information of another, with the intent that the information be used by another person to commit an unlawful act. Lists exceptions for use of personal identifying information. Defines "personal identifying information." Includes provisions regarding forfeiture and sale of goods and disposition of proceeds. Provides requirements for private entities or businesses to protect any personal identifying information contained in their records prior to discarding the records.
	§ 39-16-303	Governs the offense of using false identification for the purpose of obtaining goods, services or privileges to which a person is not otherwise entitled or eligible. Using false identification is a Class C misdemeanor.
	§§ 47-18-2101 to 47-18-2107	The Identity Theft Deterrence Act of 1999. Prohibits identity theft and unfair or deceptive practices for the purpose of engaging in identity theft. Establishes venue. Creates civil cause of action and authorizes damages, including attorney's fees and costs. Enables the Attorney General of Tennessee to initiate actions for injunctive relief and for violations of the Tennessee Consumer Protection Act of 1977.
Texas	Penal Code § 32.51	Fraudulent Use or Possession of Identifying Information. Defines "identifying information." Allows prosecution under this section or under any other applicable law. Authorizes the court to order restitution to a victim, for lost income and other expenses, excluding attorney's fees. Possession of identifying information is a state jail felony.
Utah	§§ 76-6-1101 to 76-6-1105	Identity fraud Act. Defines identity theft as when a person knowingly or intentionally obtains personal identifying information of another person and uses or attempts to use that information with fraudulent intent. Defines "personal identifying information." Classification of offenses is based on the value of the credit, goods, services, or any other thing of value. Makes the Attorney General of Utah responsible for investigating identity theft violations when identity theft is the primary violation, in addition to other law enforcement investigations. Authorizes the court to make appropriate findings regarding identity theft victims in any prosecution of such a crime, including noting that the person whose identity was falsely used to commit the crime did not commit the crime.
Vermont	Ch. 47 § 2030	Prohibits unauthorized obtaining, producing, possessing, using, selling, giving, or transferring personal identifying information belonging or pertaining to another person with intent to use the information to commit a misdemeanor or a felony. Defines "personal identifying information." Establishes as an affirmative defense consent of the person whose personal identifying information was used. Provides enhanced penalties for subsequent violations.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES ENACTED PRIOR TO 2005

State	Statute	Summary
	Ch. 63 §§ 2480h to 2480j	Authorizes identity theft victims to place a security freeze on a consumer credit report, thereby prohibiting the release of information without the written consent of the consumer. Establishes procedure for notifying credit reporting agency. Prohibits the agency from charging a fee related to a security freeze. Enumerates duties of credit reporting agency after security freeze has been imposed. Lists exemptions from requirement of placing a security freeze.
Virginia	§ 18.2-186.3	Prohibits obtaining, recording, or using identifying information of another person without permission to obtain goods, services, or identifying documents or benefits of the other person. Makes it unlawful to use the identifying documents of another person to avoid arrest or prosecution. Defines "identifying information." Classification of offenses is based on amount of financial loss and subsequent convictions. Any violation resulting in the arrest and detention of in identity theft victim whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony.
	§ 18.2-186.3:1	Authorizes consumers to request a security freeze of their consumer credit information by submitting a written request and police report to the consumer reporting agency. Provides conditions in which the consumer reporting agency may deny or rescind a credit freeze. Directs the consumer reporting agency to accept the consumer's version of disputed information and correct the disputed item in certain circumstances. Requires a consumer reporting agency to delete inquiries for credit reports based upon credit requests that the consumer reporting agency verifies were in violation of Virginia identity theft law.
	§ 18.2-186.4	Makes it unlawful for any person, with the intent to coerce, intimidate, or harass another person, to publish the person's name or photograph along with identifying information.
	§ 18.2-186.5	Authorizes the Attorney General of Virginia, in cooperation with the state police, to issue an Identity Theft Passport to identity theft victims. Describes the identity theft passport. Enables the Attorney General to provide identity theft information to criminal justice agencies and individuals who have submitted the court order.
Washington	§ 19.182.160	Requires consumer credit agencies to permanently block from reporting any information an identity theft victim identifies on his or her consumer report as being the result of identity theft. Provides exceptions for credit reporting agencies.
	§ 19.182.170	Authorizes a victim of identity theft to place a security freeze on his or her credit report. Establishes procedures for making a request. Provides exceptions for credit reporting agencies.
	§ 19.182.180	Lists information in a consumer credit report that cannot be changed without the written consent of the consumer if a security freeze is in place.
	§ 19.182.190	Provides exceptions to general applicability of credit freeze requirements.
	§ 19.182.200	Lists entities that are exempt from credit freeze requirements.
	§ 28B.10.042	Prohibits institutions of higher education from using the social security number of any student, staff, or faculty member for identification except for the purposes of employment, financial aid, research, assessment, accountability, transcripts, or as otherwise required by state or federal law. Requires development of a system of personal identifiers for students to be used for grading and other purposes.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES
ENACTED PRIOR TO 2005

State	Statute	Summary
	§§ 9.35.001 to 9.35.010	States legislative intent and defines terms. Prohibits improperly obtaining, or attempting to obtain, or causing to be disclosed or attempting to cause to be disclosed to any person, financial information from a financial institution.
	§ 9.35.020	Outlaws knowingly obtaining, possessing, using, or transferring identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime. Classification of offenses is based on aggregate value of goods, services, or anything else of value. Creates a civil cause of action for identity theft victims for damages, including costs to repair the victim's credit record and reasonable attorney's fees as determined by the court. Establishes venue as any locality where the victim resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in that locality. Authorizes the court to issue orders to correct a public record that contains false information resulting from a violation of Washington identity theft laws. Provides an exception for violations involving any person who obtains another person's driver's license or other form of identification for the sole purpose of misrepresenting his or her age.
	§ 9.35.030	Makes it unlawful for any person to knowingly use a means of identification or financial information of another person to solicit undesired mail with the intent to annoy, harass, intimidate, torment, or embarrass that person. Soliciting undesired mail is a misdemeanor. Creates civil liability for damages of $500 or actual damages, whichever is greater, including costs to repair the victim's credit record and reasonable attorney's fees as determined by the court.
West Virginia	§ 61-3-54	Prohibits knowingly taking the name, birth date, social security number, or other identifying information of another person, without the consent of that other person, for the purpose of making financial or credit transactions in the other person's name. Identity theft is a felony. Provides an exception to prosecution for identity theft for any person using a driver's license or other form of identification for the sole purpose of misrepresenting age.
Wisconsin	§ 943.201	Defines "personal identifying information" and "personal identification document." Prohibits intentionally using, attempting to use, or possessing with intent to use, any personal identifying information or personal identification document of an individual, including a deceased individual, without authorization or consent, to obtain credit, goods, services, employment, or any other thing of value, to avoid civil or criminal penalty, or to harm the reputation, property, person, or estate of the individual. Establishes as an affirmative defense that the defendant was authorized by law to engage in the conduct that is the subject of the prosecution. Directs law enforcement agencies to prepare a report when it reasonably appears that an individual's personal identifying information or personal identification documents are in the unlawful possession of another. Misappropriation of personal identifying information or personal identification documents is a Class H felony.
	§ 943.203	Prohibits intentionally using, attempting to use, or possessing with intent to use, any identifying information or identification document of an entity without authorization or consent to obtain credit, goods, services, employment, or any other thing of value, to avoid civil or criminal penalty, or to harm the reputation or property of the entity. Defines related terms. Establishes as an affirmative defense that the defendant was authorized by law to engage in the conduct that is the subject of the prosecution. The unauthorized use of an entity's identifying information or documents is a Class H felony.

APPENDIX I
COMPILATION OF STATES' IDENTITY THEFT STATUTES ENACTED PRIOR TO 2005

State	Statute	Summary
Wyoming	§ 6-3-901	Prohibits theft of identity, which is when a person willfully obtains personal identifying information of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person. Defines "personal identifying information." Classification of offenses is based on economic value gained. Authorizes restitution for any costs incurred in clearing victim's name or credit rating or in connection with debt collection proceeding arising as a result of the actions of the defendant. Directs the annotation of court records that the person whose identity was falsely used to commit a crime did not commit the crime.

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

ALASKA

S.B. 140

Prohibits spyware and unsolicited Internet advertising.

8/30/05 Signed by Governor. Chapter 97, SLA 05. Effective 11/28/05.
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

ARIZONA

H.B. 2414

Makes it unlawful to transmit, through intentionally deceptive means, computer software that modifies certain settings, collects personally identifiable information, or takes control of the computer.

04/18/05 Signed by Governor, Chapter 136
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

H.B. 2470

Imposes a $100 civil penalty on a person or entity that violates the Social Security number confidentiality restrictions. Specifies that the penalty applies to the restriction of putting a Social Security number on any card required for the individual to receive products or services provided by the person/entity. States that the penalty applies to those who knowingly or intentionally violate the restriction. Makes the penalty apply to each violation. Requires monies received from civil penalties be deposited into the state General Fund.

4/25/05 Signed by Governor, Chapter 230
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 1017

Adds premiums for long-term and critical care insurance, prepaid legal services, personal computer systems, and identity theft protection services to those payroll deductions that a state officer or employee may authorize as additional deductions.

4/18/05 Signed by Governor, Chapter 82
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 1058

Creates the crime of aggravated identity theft if a person knowingly takes, purchases, manufactures, records, possesses or uses personal identifying information of either: five or more persons or entities or a person or entity and causes a loss to a person/entity of $3,000 or more. Provides that proof of possession of the personal/entity identifying information of five or more persons/entities out of the course of regular business may give rise to an inference that the information was possessed for an unlawful purpose. Makes aggravated identity theft a Class 3 felony. Creates the crime of trafficking in the identity of another person or entity if a person knowingly sells, transfers or transmits personal/entity identifying information (real or fictitious) for an unlawful purpose or to cause loss, whether the person or entity actually suffers any economic loss. Makes trafficking in the identity of a person or entity a Class 2 felony. Exempts a violation of A.R.S. 4-241 by a person under 21 years of age from the penalties associated with identity theft (Class 4 felony), aggravated identity theft (Class 3 felony) and trafficking in the identity of another person (Class 2 felony). A.R.S. § 4-241 makes it a Class 1 misdemeanor if a person under 21 years old uses a fraudulent piece of identification to gain access to an establishment licensed to sell liquor.

4/25/05 Signed by Governor, Chapter 190
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 1447

Prohibits the solicitation of an individual's identifying information via a web page or e-mail by a person representing they are an on-line business who has not been approved to do so by the business they are representing and establishes civil penalties and damages.

04/18/05 Signed by Governor, Chapter 114
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

ARKANSAS

H.B. 1106

Creates the Student Identity Protection Act; prohibits the use of a student's Social Security number as a student identification number.

2/22/05 Signed by Governor, Act 246
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1117

Amends the petition form for an order of protection to eliminate any requirement for disclosure of Social Security numbers.

2/1/05 Signed by Governor, Act 55
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

H.B. 1354

Clarifies that the offense of financial identity fraud pertains to the use of identifying information to open or create an account or financial resource.

2/25/05 Signed by Governor, Act 280
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 1740

Provides for the issuance of an identity theft passport by the attorney general to victims of financial identity fraud.

3/10/05 Signed by Governor, Act 744
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2094

Prohibits persons convicted of financial identity fraud from being eligible to work with the developmentally disabled.

3/21/05 Signed by Governor, Act 968
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2261

An act to make an appropriation for expenses associated with spyware monitoring for the office of Attorney General.

04/14/05 Signed by Governor, Act 2312
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

H.B. 2344

An act to make an appropriation for expenses associated with spyware monitoring for the Department of Information Systems.

04/14/05 Signed by Governor, Act 2313
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

H.B. 2619

Amendment to include the use of a scanning device or re-encoder in the offense of financial identity theft.

Act 1018
Westlaw
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2706

Amend Arkansas laws concerning the use of Social Security numbers in pleadings, motions, and decrees.

4/8/05 Signed by Governor, Act 1877
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 2849

Act to protect military records filed with county recorder from identity theft.

Approved 4/13/2005, Act 2249
Westlaw
Enacted Identity Theft Legislation - 2005 Session (current through 10/25/2005)

H.B. 2904

Establishes the Consumer Protection Against Computer Spyware Act.
Prohibits specified uses of computer spyware; prohibits phishing, brand spoofing or carding.

04/15/05 Signed by Governor, Act 2255
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing," Spyware or Adware (current through 10/25/2005)

S.B. 1167

Creates the Personal Information Protection Act; provides notice to consumers of the disclosure of their personal information.

4/4/05 Signed by Governor, Act 1526
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

S.B. 335

Prevents the misappropriation of Social Security numbers.

3/30/05 Signed by Governor, Act 1295
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

CALIFORNIA

A.B. 1741

Prohibit the requester of voter information or of signatures or other information collected for an initiative, referendum, or recall petition from sending the information outside of the United States, as specified, and would state findings and declarations regarding the protection of voter-related identities and personal information of Californians.

2188.5. (a) A person who requests voter information pursuant to Section 2188 or who obtains signatures or other information collected for an initiative, referendum, or recall petition shall not send that information outside of the United States or make it available in any way electronically to persons outside the United States, including, but not limited to, access over the Internet

Filed with secretary of state 7/25/2005.
Westlaw
Enacted Identity Theft Legislation - 2005 Session

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

A.B. 988

Existing law specifies various offenses for purposes of defining criminal profiteering activity, and patterns of criminal profiteering activity. Existing law also provides for the forfeiture of specified assets for persons who engage in a pattern of criminal profiteering activity, upon conviction of an underlying offense, as specified. This bill adds to those specified offenses, the offense of theft of personal identifying information, as specified.

7/18/05 Signed by Governor, Chapter 53
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

AB 1556 Ch. 432, Statutes of 2005

Amends existing statute to increase the penalties for identity theft offenses involving a member of the armed forces, reserves, or National Guard.

Approved by governor 9/30/05. Ch. 432, Statutes of 2005. Effective January 1, 2006.
Report of legislation enacted in 2005 provided to the Task Force by Marvin Dang
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 355

Makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be an online business without the approval or authority of the online business. The bill would enact certain civil remedies.

09/30/05 Approved by Governor, Chapter 437, Statutes of 2005
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

SB 101

Clarifies that an employer, by January 1, 2008, may include on the itemized statement provided to an employee only the last 4 digits of the employee's social security number or employee identification number. Imposes similar requirement on any government entity.

Approved by governor 7/21/05. Chapter 103, Statutes of 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Enacted Social Security Numbers Legislation - 2005 Session

COLORADO

H.B. 1347

Concerns criminal penalties for the use of electronic devices for the purpose of identity theft.

06/01/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

S.B. 137

Permits a consumer to put a security freeze on his or her credit report. Allows the consumer to temporarily lift the security freeze to allow a particular entity access to the credit report for the purpose of issuing or extending credit to the consumer. Requires a consumer reporting agency to maintain the security freeze until the consumer specifically requests its removal. Allows a consumer reporting agency to charge a fee for temporarily or permanently lifting the security freeze. Requires that a consumer be notified of the right to place a security freeze on his or her credit report each time the consumer receives a summary of the rights relating to credit reports. Allows a consumer to bring a private civil right of action or arbitration against a consumer reporting agency that releases credit information in violation of a security freeze. Permits the secretary of state to remove personal identifying information from publicly accessible documents maintained by the secretary of state. Makes theft of personal identifying information, with the intent to defraud, from a trash receptacle a class 1 misdemeanor if the person unlawfully enters the trash receptacle.

6/1/05 Signed by Governor, Chapter 226
National Conference of State Legislatures
Consumer Report Security Freeze Legislation and Identity Theft Legislation (current through 10/25/2005)

CONNECTICUT

H.B. 6831

Specifically provides that the state statutes concerning financial privacy do not prevent 1) the disclosure of information to information networks accessed by financial institutions, other commercial enterprises and law enforcement authorities for the purpose of detecting or preventing against fraud, and 2) disclosures made to a victim of identity theft pursuant to the federal Fair Credit Reporting Act.

5/19/05 Signed by Governor, Act 05-62
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

P.A. 05-23

Prohibits the use of the name or trademark of a bank or any of its affiliates in any commercial advertisement or solicitation for goods, products, or services in a manner that misleads consumers as to the relationship between the bank or its affiliates and the person who uses such name or trademark.

Effective October 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

S.B. 650

Requires any credit bureau doing business in the state to enable residents to place a security freeze on the issuance of their credit report in order to prevent potential fraudulent access to an individual's credit report. Such freeze would enable the resident to authorize the bureau to release the credit report to a potential lender, employer or landlord if such lender, employer or landlord was provided with a personal identification number by such resident.

6/8/05 Enacted, Public Act 05-148
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

DELAWARE

S.B. 50

Provides that a person is guilty of the crime of possession of burglar's tools or instruments facilitating theft when the person possesses any tool, instrument, or other thing adapted, designed, or commonly used for committing or facilitating the offense of identity theft, such as a credit card, driver license or other document issued in a name other than the name of the person who possesses the document.

7/12/05 Signed by Governor, Chapter 162
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

FLORIDA

H.B. 1591

Exempts a voter's Social Security number and signature from the public records laws.

6/20/05 Signed by Governor, Chapter 279
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1695

Provides that individual records of a child enrolled in the Voluntary Prekindergarten Education Program held by an early learning coalition, the Agency for Workforce Innovation, or a Voluntary Prekindergarten Education Program provider be made confidential and exempt from public records requirements. The exemption includes assessment data, health data, records of teacher observations, and personal identifying information of an enrolled child and his or her parent,.

6/20/05 Signed by Governor, Chapter 279
Westlaw
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1817

Removes the October 2, 2005, repeal of information regarding an active investigation or office review of certified capital company scheduled under OGSR Act; eliminates the exemption from public-records requirements for Social Security numbers of any customers of certified capital company, complainants, or persons associated with said company or qualified business.

5/26/05 Signed by Governor, Chapter 91
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 481

Relates to the unlawful use of personal identification information; includes other information within the definition of the term "personal identification information"; defines the term "counterfeit or fictitious personal identification information"; revises criminal penalties regarding the offense of fraudulently using, or possessing with intent to fraudulently use, said information; requires business persons maintaining computerized data that includes personal information to provide notice of breaches of system security.

6/14/05 Signed by Governor, Chapter 229
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

GEORGIA

H.B. 437

Relates to exceptions from the requirements of public disclosure, so as to exempt disclosure of certain personal information, including Social Security numbers, of public employees.

5/2/05 Signed by Governor, Act 105
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 127

Relates to forgery and fraudulent practices, so as to enact the "Georgia Computer Security Act of 2005." Prohibits certain deceptive acts and practices with regard to computers; requires certain notices be given prior to certain software or programs being loaded onto certain computers; requires certain functions be available in certain software; provides for certain exceptions; provides for civil and criminal penalties; provides for recovery of certain damages.

05/10/05 Signed by Governor, Act 389
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

S.B. 230

Relates to selling and other trade practices, so as to provide definitions; requires investigative consumer reporting agencies to give notice to consumers of certain security breaches.

5/5/05 Signed by Governor, Act 163
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

SB 62

Creates the new crime of initiation of deceptive commercial email, defined as initiating an email the sender knew or should have known to be false and misleading.

Signed by governor 4/19/05, Act 46. Effective July 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Deceptive Commercial Email

HAWAII

H.B. 119

Allows only the last four digits of a registered voter's Social Security number on nomination papers filed on behalf of a candidate.

4/19/05 Signed by Governor, Act 13
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 553

S.B. 662

Allows government agencies to withhold personal information contained in final opinions or orders made in the adjudication of cases where the disclosure of the information would be an unwarranted invasion of personal privacy. Excludes Social Security number information of an individual under contract with the government from disclosure.

5/31/05 Signed by Governor, Act 85
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

S.B. 1170

Establishes a Hawaii anti-phishing task force to curtail electronic commerce-based criminal activities. Requires the task force to submit a report and make recommendations prior to the 2006 regular session.

05/19/2005 Signed by Governor, Act 65
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

IDAHO

H.B. 88

Proposes the Financial Fraud Prevention Act to authorize the Department of Finance to investigate and bring civil enforcement actions against perpetrators of fraud against financial institutions, including non-depository institutions, and their customers. Allows referrals of actions to criminal law enforcement agencies.

Signed by governor 4/5/05, Session Law Chapter 256. Effective July 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Financial Fraud Prevention

S.B. 1156

Amends existing law to provide that it is unlawful for any person to falsely assume or pretend to be a member of the armed forces of the United States or an officer or employee acting under authority of the United States or any department, agency or office thereof or of the state of Idaho or any department, agency or office thereof, and in such pretended character, seek, demand, obtain or attempt personal identifying information of another person; and provides felony penalties for such action.

3/31/05 Signed by Governor, Chapter 219
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

ILLINOIS

H.B. 1058

Amends the Consumer Fraud and Deceptive Business Practices Act. Provides that a consumer who has been the victim of identity theft may place a security freeze on his or her credit report by making a request in writing by certified mail to a consumer credit reporting agency with a valid copy of a police report, investigative report, or complaint that the consumer has filed with a law enforcement agency about unlawful use of his or her personal information by another person. Requires a credit reporting agency to place a security freeze on a consumer's credit report no later than five business days after receiving a written request from the consumer. Provides that if the consumer wishes to allow his or her credit report to be accessed for a specific party, parities, or period of time while a freeze is in place, he or she shall contact the consumer credit reporting agency, request that the freeze be temporarily lifted, and provide certain information. Provides that if a security freeze is in place, a credit reporting agency shall not change any of the following official information in a credit report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file: (i) name, (ii) date of birth, (iii) Social Security number, and (iv) address. Provides that certain entities are not required to place a security freeze in a credit report provided certain conditions are met. Defines "proper identification."

6/24/05 Signed by Governor, Public Act 94-0074
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

H.B. 173

Amends the Income Withholding for Support Act. Provides that the court, at its discretion, may withhold the Social Security numbers of the child or children from being disclosed in the income withholding notice.

6/17/05 Signed by Governor, Public Act 94-0043
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 265

Amends the Use of Credit Information in Personal Insurance Act. Defines extraordinary life events to include identity theft.

7/19/05 Signed by Governor, Public Act 94-0245
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

H.B. 2696

Provides that it is an unlawful practice for a person to deny credit or public utility service to or reduce the credit limit of a consumer solely because the consumer has been a victim of identity theft, if the consumer i) has provided a copy of an identity theft report as defined under the federal Fair Credit Reporting Act and implementing regulations (instead of a police report) evidencing the consumer's claim of identity theft; ii) has provide d a properly completed copy of a standardized affidavit of identity theft or an affidavit of fact that is acceptable to the person for that purpose; iii) has obtained placement of an extended fraud alert in his or her file maintained by a nationwide consumer reporting agency, in accordance with the requirements of the federal Fair Credit Reporting Act; and iv) is able to establish his or her identity and address to the satisfaction of the person providing credit or utility services.

6/16/05 Signed by Governor, Public Act 94-0037
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2697

Amends the Criminal Code of 1961. Provides that a person who is not a party to a transaction that involves the use of a financial transaction device may not secretly or surreptitiously photograph, or otherwise capture or record, electronically or by any other means, or distribute, disseminate, or transmit, electronically or by any other means, personal identifying information from the transaction without the consent of the person whose information is photographed, or otherwise captured, recorded, distributed, disseminated, or transmitted. Provides that a violation is a Class A misdemeanor.

6/16/05 Signed by Governor, Public Act 94-0038
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2697

Amends the Criminal Code of 1961 to protect personal identifying information from being secretly or surreptitiously recorded, photographed, transmitted, distributed, or otherwise disseminated. Provides that a violation is a Class A misdemeanor.

Approved by the governor 6/16/05, House Public Act 94-0038. Effective immediately.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

H.B. 2699

Amends the Criminal Code of 1961. Increases the penalties for identity theft and aggravated identity theft by one class higher than the current law.

6/16/05 Signed by Governor, Public Act 94-0039
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

H.B. 2700

Amends the Criminal Code of 1961. Provides that a person who commits the offense of identity theft or aggravated identity theft may be tried in any one of the following counties in which: 1) the offense occurred; 2) the information used to commit the offense was illegally used; or 3) the victim resides. Provides that if a person is charged with more than one violation of identity theft or aggravated identity theft and those violations may be tried in more than one county, any of those counties is a proper venue for all of the violations.

6/17/05 Signed by Governor, Public Act 94-0051
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 457

Provides that a prosecution for identity theft or aggravated identity theft may be commenced at any time (rather than within one year and six months after the commission of the offense if it is misdemeanor identity theft and within three years after commission of the offense if it is felony identity theft or aggravated identity theft).

7/19/05 Signed by Governor, Public Act 94-0253
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 123

Amends the Illinois Administrative Procedure Act and the Department of Natural Resources Act. Requires the Department of Natural Resources as soon as practicable to assign a customer identification number to each applicant for a hunting or fishing license. Provides that after the applicant has been assigned a customer identification number, the applicant may use that customer identification number in place of his or her Social Security number on any subsequent application for a hunting or fishing license. Requires the Department to keep a record of the Social Security number of each applicant and to notify each applicant that his or her Social Security number is kept on file with the Department. Provides that a licensee's Social Security number shall not appear on the face of his or her hunting or fishing license.

6/16/05 Signed by Governor, Public Act 94-0040
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 1799

Amends the Department of Revenue Law of the Civil Administrative Code of Illinois. Requires the Department of Revenue to notify an individual if the Department discovers or reasonably suspects that another person has used that individual's Social Security number.

6/16/05 Signed by Governor, Public Act 94-0041
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

INDIANA

H.B. 1073

Specifies that: (1) the Bureau of Motor Vehicles (Bureau) has discretion to withhold certain medical records and evaluations regarding the ability of a driver to operate a motor vehicle safely; and (2) a law enforcement agency has discretion to withhold certain items of personal information contained in the files of the law enforcement agency. Exempts a Social Security number contained in the records of a public agency from disclosure.

5/11/05 Signed by Governor, Public Law No. 210
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 227

Prohibits the Bureau of Motor Vehicles from placing a Social Security number on certain identifying documents without authorization from the holder of the identifying documents. Requires the Bureau to adopt rules that do not require the Social Security number of the holder of a commercial driver's license to be contained on the license.

5/4/05 Signed by Governor, Public Law No. 123
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 503

Prohibits a state agency from releasing the Social Security number of an individual unless the release is: (1) required by state law, federal law, or court order; (2) authorized in writing by the individual; (3) made to comply with the USA Patriot Act or Presidential Executive Order 13224; or (4) made to a commercial entity for permissible uses set forth in the Drivers Privacy Protection Act, the Fair Credit Reporting Act, or the Financial Modernization Act of 1999. Provides that disclosure of the last four digits of a Social Security number is not considered a disclosure of the Social Security number. Requires a state agency to notify an individual of a security breach of the agency's computer system if the individual's unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Makes it a Class D felony to knowingly make a false representation to obtain a Social Security number or for an agency employee to knowingly disclose a Social Security number. Provides that an agency employee who negligently discloses a Social Security number commits a Class A infraction. Requires an individual who prepares a document for recording to certify that the individual reviewed the entire document and took reasonable care to redact Social Security numbers in the document. After December 31, 2007, requires a county recorder or an employee of a county recorder to search documents using redacting technology to redact Social Security numbers before the documents are release for public inspection. Authorizes establishment of a pilot project beginning July 1, 2005, to develop procedures and test technology and equipment for searching recorded documents and redacting Social Security numbers. Requires county recorders to seek federal grants, private funds, and other sources of money to implement redacting technology.

4/26/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

SB 49

Prohibits the transmission or installation of spyware, as defined in the Act. Authorizes a provider of computer software, a web site owner, or a trademark or copyright holder harmed by a prohibited use of spyware to bring a civil action against the perpetrator. Allows injunctive relief and the greater of actual damages or $100,000 in causes of action for unlawful spyware installation.

PL 115-2005. Effective July 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Spyware

IOWA

H.F. 614

Protects owners and operators of computers from the use of spyware and malware that is deceptively or surreptitiously installed on the owner's or the operator's computer.

05/03/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

S.F. 270

Relates to identity theft including criminal violations and damages recoverable in a civil action, provides for forfeiture of property and for certain rights of financial institutions, and provides for civil remedies.

4/6/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.F. 74

Prohibits the misleading and deceptive use of a financial institution's or insurer's name, trademark, logo, or symbol. Allows financial institutions or appropriate state regulator to bring an action to enjoin the prohibited use.

Signed by governor 4/13/05, S.J. 875. Effective July 2, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

KANSAS

H.B. 2087

Changes the definition of identity theft from someone who uses personal identification to knowingly and intentionally defraud a person for economic benefit, to a person receiving any benefit from using someone else's personal identification. Establishes identity theft for economic benefit as a severity level 7 person felony, and identity theft for non-economic benefit as a class A non-person misdemeanor under Kansas criminal code.

4/13/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

SB 2205

Prohibits the inclusion of an actual or similar name, trade name, or trademark of a lender in a solicitation for products or services without the consent of the lender, unless it conspicuously states in boldface type on the front page that the person is not affiliated with, sponsored or authorized by, the lender.

Approved by governor 4/4/05, H.J. 888. Effective July 7, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

LOUISIANA

H.B. 214

Provides that the recorder of documents will only display the last four digits of the social security numbers listed on instruments that the office makes available for viewing.

Signed by governor 6/28/05, Act 169. Effective January 1, 2006.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Enacted Social Security Numbers Legislation - 2005 Session

MAINE

L.D. 464

Amends existing statute to prohibit using the name of a financial institution in the solicitation of insurance without its express written permission, unless the person discloses that permission has not been granted and that there is no affiliation with the financial institution.

Signed by governor 4/8/05, Public Law Ch. 46. Effective upon approval.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

L.D. 581

Prohibits a consumer reporting agency from furnishing a consumer report or disclosing information about a consumer unless the consumer has authorized the disclosure if the consumer has given a copy of a police report to the consumer reporting agency that was prepared by a law enforcement agency in an investigation of identity theft involving the consumer.

5/26/05 Signed by Governor, Chapter 243
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

MARYLAND

H.B. 56

Prohibits the public posting or displaying of an individual's Social Security number under specified circumstances; prohibits the printing of an individual's Social Security number on specified cards under specified circumstances; prohibits a person from requiring an individual to transmit the individual's Social Security number over the Internet under specified circumstances; prohibits a person from transmitting an individual's Social Security number over the Internet under specified circumstances.

5/26/05 Signed by Governor, Chapter 521
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 800

Requires a local law enforcement agency, after being contacted by a person who knows or reasonably suspects that the person is a victim of identity fraud, to promptly prepare and file a report of the alleged identity fraud and provide a copy of the report to the victim.

5/26/05 Signed by Governor, Chapter 579
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 818

Establishes a Task Force to Study Identity Theft; specifies the membership and duties of the Task Force; provides for the appointment of a Senate co-chairman and House co-chairman of the Task Force; provides for the staffing of the Task Force; prohibits a member of the Task Force from receiving compensation for serving on the Task Force; authorizes a member of the Task Force to receive reimbursement; requires a report to the General Assembly by December 31, 2006.

4/26/05 Signed by Governor, Chapter 241
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 43

Establishes a Task Force to Study Identity Theft; specifies the membership and duties of the Task Force; provides for the appointment of a Senate co-chairman and House co-chairman of the Task Force; provides for the staffing of the Task Force; prohibits a member of the Task Force from receiving compensation for serving on the Task Force; authorizes a member of the Task Force to receive reimbursement for specified expenses; requires a report to the General Assembly on or before December 31, 2006.

4/23/05 Signed by Governor, Chapter 242
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

MINNESOTA

H.F. 1

Prohibits a person, with intent to obtain another's identity, from using false pretense in an e-mail, Web page, or any other Internet communication. This offense is punishable by five years imprisonment and/or a $10,000 fine. In prosecution under this section, it is not a defense that the person did not obtain or use another's identity, nor is it a defense that the crime did not result in a loss to any person.

06/02/05, Signed by Governor, Chapter 136
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

H.F. 1385

Requires the Higher Education Services Office to consider developing data collection procedures and agreements using the students' Social Security numbers to monitor the extent to which students who attend Minnesota postsecondary institutions under reciprocity agreements are employed in Minnesota after graduation.

5/26/05 Signed by Governor, Chapter 107
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.F. 225

Makes technical, conforming, and clarifying changes to the Minnesota Government Data Practices Act; defines terms; classifies, regulating, and reviewing access to and dissemination of certain data; provides notice of breaches in security; regulates certain fees; provides for the conduct of certain board and council meetings; modifies provisions regulating motor vehicle and driver applications and records; regulates disclosure of non-identifying sales tax returns; modifies vehicle accident reports and procedures; provides for treatment of data held by the comprehensive incident-based reporting system; regulates use of Social Security numbers; classifies certain animal health data; defining terms and regulates data privacy practices for wireless telecommunications; providing for a review of the handling of genetic information.

6/3/05 Signed by Governor, Chapter 163
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

MISSOURI

H.B. 353

Prohibits requiring an individual to use his or her social security number as an employee number for any type of employment.

Approved 7/13/2005.
Westlaw
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 353

Amends Penalties: Class C felony resulting in theft changed from $500 and not exceeding ten thousand dollars to not excceding ive thousand dollars. Class B felony resulting in theft changed from five thousand dollars and not exceeding one hundred thousand dollars to not exceeding fifty thousand dollars. Class A felony resulting in theft changed from exceeding one hundred thousand dollars to exceeding fifty thousand dollars.

Approved 7/13/2005.
Westlaw
Enacted Identity Theft Legislation - 2005 Session (current through 10/25/2005)

MONTANA

H.B. 110

Creates an identity theft passport program.

3/24/05 Signed by Governor, Chapter 55
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 732

Adopts and revises laws to implement individual privacy and to prevent identity theft; requires a consumer reporting agency to block or expunge information on a report that results from a theft of identity; provides privacy protection provisions for credit card solicitations and renewals and telephone accounts; provides privacy protection for business records by requiring destruction of records; requires businesses to report a breach of computer security; requires a business that has an established business relationship with a customer and that has disclosed certain personal information to third parties to report that information to the customer; providing remedies and penalties for violation.

4/28/05 Signed by Governor, Chapter 518
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

S.J.R. 38

Designates interim committee pursuant to section 5-5-217, MCA, or direct sufficient staff resources to study issues related to identity theft.

File with secretary of state on 4/25/2005.
Westlaw
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

NEVADA

A.B. 1, Special Session

Changes the effective date for A.B. 334 and amends the definition of personal information in S.B. 347.

6/17/05 Signed by Governor, Chapter 6
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

A.B. 334

Requires a governmental entity, except in certain circumstances, to ensure that Social Security numbers in its books and records are maintained in a confidential manner; prohibits the inclusion of Social Security numbers in certain documents that are recorded, filed or otherwise submitted to a governmental agency; requires a governmental agency or certain persons who do business in this state that own, license or maintain computerized data to notify certain persons if personal information included in that data was, or is reasonably believed to have been, acquired by an unauthorized person; expands the types of prohibited computer contaminants to include spyware.

6/17/05 Signed by Governor, Chapter 486
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

S.B. 164

Protects the confidentiality of certain personal identifying information of parents and children involved in paternity cases by removing the requirement that the court include such information in its orders which are available to the public. However, the court must continue to obtain and provide certain personal identifying information to the Welfare Division and must ensure that the Social Security numbers of parents and children that are placed in the court's records are kept confidential unless otherwise required by statute.

5/12/05 Signed by Governor, Chapter 90
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 304

Authorizes the attorney general to issue identity theft passports to victims of identity theft; prescribes the manner in which victims of identity theft may use such passports; requires the attorney general to adopt regulations relating to the issuance of identity theft passports; authorizes the attorney general to accept gifts, grants and donations to carry out the provisions relating to the issuance of identity theft passports; makes an appropriation.

6/8/05 Signed by Governor, Chapter 321
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 347

Relates to personal identifying information; prohibits the establishment or possession of a financial forgery laboratory; enhances the penalties for crimes involving personal identifying information that are committed against older persons and vulnerable persons; requires the issuer of a credit card to provide a notice including certain information concerning its policies regarding identity theft and the rights of cardholders when issuing a credit card to a cardholder; requires data collectors to provide notification concerning any breach of security involving system data; making various other changes concerning personal identifying information; provides penalties; and provides other matters properly relating thereto.

6/17/05 Signed by Governor, Chapter 485
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 80

Allows a consumer to ask a credit reporting agency to place a security freeze on his consumer report. A security freeze prohibits the release of a consumer report to most other persons without the express authorization of the consumer. Exempts certain companies that issue reports on fraud and certain resellers of credit information from the requirement to place a security freeze on a consumer report. Allows a credit reporting agency to release a consumer report to governmental agencies and certain other persons for specific purposes even though a security freeze is in place.

6/13/05 Signed by Governor, Chapter 391
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

NEW HAMPSHIRE

H.B. 47

This bill regulates the use of computer spyware software that creates advertisements on a computer as a result of visiting certain Internet websites and that collects information regarding the computer's Internet use. The bill prohibits installation of spyware on another person's computer.

07/14/05 Signed by Governor, Chapter 238
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

NEW JERSEY

A.B. 1205

S.B. 1636
Substituted by A.B. 1205 12/13/04
Prohibits public or independent institutions of higher education in the state from displaying any student's Social Security number to identify that student for posting or public listing of grades, on class rosters or other lists provided to teachers, on student identification cards, in student directories or similar listings, unless otherwise required in accordance with applicable state or federal law.

1/26/05 Signed by Governor, Chapter 28
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

A.B. 2047

Prohibits any person, including any public or private entity, from printing or displaying in any manner an individual's Social Security number on any document intended for public recording with any county recording authority. Provides that, in the case of certain documents, the county recording authority is authorized to delete, strike, obliterate or otherwise expunge a Social Security number that appears on the document without invalidating it. As specified in the bill, the fact that such a document is recorded without deleting, striking, obliterating or otherwise expunging that Social Security number shall not render the document invalid, void, voidable or in any way defective. Court documents, tax documents, documents that constitute non-consensual liens against an individual, documents required to contain a Social Security number by law, and documents filed with the County Surrogate are exempt and county recording authorities, therefore, may not make any changes on them.

6/15/05 Signed by Governor, Chapter 99
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

A.B. 4001

A sweeping identity theft bill containing provisions relating to notice of security breach, police reports, consumer security freezes, and restricting use of social security numbers.

Approved 9/24/05, P.O. 2005, c. 226. Effective date to be determined.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
2005 Enacted Identity Theft Legislation

S.B. 2665

Allows victims of identity theft to obtain an official incident report from their local law enforcement agency. Establishes a procedure for a factual determination of innocence. After an order is entered, a court may seal or delete the name and personal identifying information of a victim contained in court records, files and indexes, or add a label to show that the data does not reflect the defendant's identity. Requires creation and maintenance of an identity theft victims data base and toll-free information number Amends and supplements the "New Jersey Fair Credit Reporting Act," to allow consumer credit report security freezes. Prohibits certain uses or disclosures of an individual's social security number

9/22/05 Signed by Governor, P.L. 2005, c. 226
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

NEW MEXICO

S.B. 720

Amends the existing identity theft statute to include the new crime of obtaining identity by electronic fraud. Obtaining information by electronic fraud (commonly known as phishing) is defined as using an e-mail web site or other means of electronic communication to obtain personal information by false pretenses. This new crime is a fourth degree felony. This act also adds a section giving a civil remedy for victims of ID theft or fraud.

04/07/05 Signed by Governor, Chapter 296
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

NORTH CAROLINA

S.B. 1048

Enacts the Identity Theft Protection Act of 2005, including consumer report security freezes and protections for Social Security numbers.

9/21/05 Signed by Governor, SL 2005-414
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

NORTH DAKOTA

H.B. 1211

Relates to unauthorized use of personal identifying information of a deceased individual; and provides a penalty.

3/30/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 1500

Provides for protection of victims of identity fraud; and provides a penalty.

Signed by Governor 4/22/05. Chapter 448
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 2251

Relates to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; relates to the unauthorized use of personal identifying information, penalties, and prosecution of offenses in multiple counties; jurisdiction in offenses involving conduct outside this state; and provides a penalty.

4/22/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

OHIO

H.B. 48

Increases the penalty for identity fraud in certain circumstances, including when it is committed against an elderly person or disabled adult, modifies the affirmative defenses available for that offense, and creates the Identity Fraud Passport.

6/14/05 Signed by Governor, Session Law 22
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

RHODE ISLAND

H.B. 6191

Creates the "Rhode Island Identity Theft Protection Act of 2005", and establishes standards for such protection, and provides for penalties for violations of the act.

7/10/05 Effective without Governor's signature, Public Law 225
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

SOUTH DAKOTA

S.B. 129

Prohibits the display of Social Security numbers on driver licenses or non-driver identification cards.

2/23/05 Signed by Governor
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

TENNESEE

H.B. 1095

Prohibits the display of more than five digits of a credit or debit card or the expiration date upon either the receipt retained by merchant or receipt provided to cardhold at point of sale.

Approved 5/13/2005. Pub. Ch. 161
National Conference of State Legislatures
Enacted Identity Theft Legislation - 2005 Session (current through 10/25/2005)

TEXAS

H.B. 1098

Relating to using the Internet to obtain identifying information of another person for a fraudulent purpose; providing penalties.

06/17/2005 Signed by Governor, Chapter 544
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

H.B. 1130

Relates to the adoption of a privacy policy by a person who requires the disclosure of an individual's Social Security number.

5/27/05 Signed by Governor
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1368

Relates to the confidentiality of and access to certain personal information, such as Social Security numbers, in instruments recorded with a county clerk.

5/13/05 Signed by Governor
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1379

Makes communications by a seller of goods or services to a member of a law enforcement agency regarding an investigation of an identity theft violation inadmissible in a civil action.

6/18/05 Signed by Governor, Chapter 1059
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 2191

Provides that the Social Security number of a living person is excepted from the requirements of Section 552.021, Government Code. Allows a governmental body to redact the Social Security number of a living person from any information the governmental body discloses without the necessity of requesting a decision from the attorney general.

Signed by Governor 6/17/05
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 2223

Provides that if an account with a financial institution is closed because of identity theft, the financial institution must take certain measures in connection with checks and documents subsequently drawn on the closed account.

Signed by governor 6/17/05. Effective September 1, 2005.
List of state legislation enacted in 2005 compiled from charts provided to the Task Force by Marvin Dang (current through 2005 Enacted Identity Theft Legislation

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

H.B. 3212

Prohibits a lender or any other person involved in a transaction from denying credit or loans or restricting or limiting the credit extended to a person based on the person being a victim of identity theft. Provides victims of identity theft with another tool to mend their credit histories and bring state law in line with the Federal Equal Credit Opportunity Act, which prohibits creditors from discriminating against credit applicants who exercise their rights, in good faith, under the Fair Credit Billing Act.

5/20/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

H.B. 698

Provides for the disposal of business records that contain personal identifying information as defined by this section. A business that does not properly dispose of a business record that contains personal identifying information of a customer is liable for a civil penalty of up to $500 for each record. A business that modifies a record in good faith is not liable for a civil penalty. Grants the attorney general authority to bring suit against the business to recover a civil penalty, obtain any other remedy, including injunctive relief, as well as costs and attorney's fees.

6/18/05 Signed by Governor
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 853

Prohibits the collection of identifying information from a consumer for use in compiling or tracking their returns of merchandise. Grants the attorney general, or the county attorney, authority to bring suit to recover a civil penalty of up to $500 for each violation. The attorney general has authority to restrain or enjoin a person from violating this section.

6/18/05 Signed by Governor
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 982

Relates to posting a sign warning restaurant or bar employees against fraudulent use or possession of identifying information; provides a criminal penalty.

5/27/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

S.B. 122

Amends the Code of Criminal Procedure by requiring that a peace officer to whom an alleged violation of identity theft is reported make a written report that includes the name of the victim, suspect, if known, type of identifying information obtained, possessed, transferred, or used, and the results of the investigation. Sets forth provisions for prevention and punishment of identity theft and assistance to certain victims of identity theft. Imposes a civil penalty of at least $2,000 but not more than $50,000 for each identity theft violation and authorizes the attorney general to bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or a permanent or temporary injunction. Gives the attorney general the option to file in a district court in Travis County or in any county in which the offense occurred or where the victim lives. Authorizes the attorney general to recover reasonable expenses incurred in obtaining injunctive relief and civil penalties. Penalties collected by the attorney general under this section would be required to be deposited into the General Revenue Fund and could be appropriated only for the investigation and prosecution of other cases under Chapter 48 of the Code of Criminal Procedure. Sets out that no bond is required and gives the court authority to grant other equitable relief to protect victims. Gives a victim the option to file an application with the district court for the issuance of a court order to declare them a victim of identity theft. Information contained in the court order would be considered confidential.

6/17/05 Signed by Governor
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 327

Relates to the unauthorized collection and transmission of certain information by computer; providing a penalty.

06/17/05 Signed by Governor, Chapter 298
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

S.B. 450

Relates to the confidentiality of certain personal information, including Social Security numbers, regarding the employees of a prosecutor's office.

Signed by Governor 6/17/05
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

SB 461

Requires that any instrument transferring an interest in real property that contains a social security number include a notice that state's the individual's right to strike the number before the instrument is filed.

Signed by governor 5/13/05. Effective May 13, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Enacted Social Security Numbers Legislation - 2005 Session

SB 99

Prohibits a lender from denying credit, or restricting or limiting extended credit, because a person has been the victim of identity theft. Authorizes the issuance of identity theft insurance.

Signed by governor 5/20/05. Effective September 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

UTAH

H.B. 104

This bill amends the Spyware Control Act. IT prohibits certain uses of pop-up advertisements; prohibits the purchase of pop-up advertisements that violate the chapter if the purchaser has actual notice of the violation; provides for the permissive removal of certain software; and defines the scope of actions and penalties authorized by the chapter.

03/17/05 Signed by Governor, Chapter 168
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

S.B. 118

Includes the personal identifying information of persons who are deceased in the statute that prohibits the use of identifying information to commit identity fraud crimes.

3/11/05 Signed by Governor, Chapter 101
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

VERMONT

H. 516

Creates a Social Security Usage Study Commission to study security breaches and develop proposals for effectively notifying consumers. The Commission also shall study the use of social security number by public and private entities and develop proposals for reducing such use and protecting privacy.

Signed by governor 6/21/05, Act 71. Effective July 1, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)
Enacted Social Security Numbers Legislation - 2005 Session

VIRGINIA

H.B. 2215

Modernizes the Virginia Computer Crimes Act by updating definitions to comport with changing technology, removing superfluous language and relocating language. The bill adds unauthorized installation of software on the computer of another, disruption of another computer's ability to share or transfer information and maliciously obtaining computer information without authority as additional crimes of computer trespass, a Class 1 misdemeanor.

04/04/05 Signed by Governor, Chapter 812
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

H.B. 2471

Adds as a new Class 6 felony using a computer to fraudulently gather identifying information of another (phishing), unless the information is sold or distributed to another or the information is used in the commission of another crime, in which case it is a Class 5 felony.

03/26/05 Signed by Governor, Chapter 827
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

H.B. 2482

Prohibits any person from (i) intentionally communicating an individual's Social Security number to the general public; (ii) printing an individual's Social Security number on any card required for the individual to access or receive products or services; (iii) requiring an individual to use his Social Security number to access an Internet website, unless an authentication device is also required; or (iv) mailing a package with the Social Security number visible from the outside. Exempts public bodies and public records. A violation is a prohibited practice under the Virginia Consumer Protection Act. The measure also requires the state employee's health insurance plan to use identification numbers that are not the employee's Social Security number.

Signed by Governor 3/23/05, Chapter 640
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 2631

Revises provisions in the Virginia Computer Crimes Act relating to computer fraud and redefines computer invasion of privacy by including the unauthorized gathering of identifying information and punishes subsequent offenses and transferring the information to another or use of the information in the commission of another crime as a Class 6 felony. Currently, the offense is punishable as a Class 1 misdemeanor. Additionally, the fraudulent gathering of such information is punished as a Class 6 felony, a new crime, and transferring the information to another or use of the information in the commission of another crime is a Class 5 felony.

04/04/05 Signed by Governor, Chapter 837
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

S.B. 1019

Requires that the record of any divorce suit not contain the Social Security number of any party or of any minor child, or any financial information. If such information must be provided to a government agency or recorded for the benefit of the parties, it shall be contained in a separate addendum. The addendum can be used to distribute the information as required by law but shall otherwise be made available only to the parties, their attorneys, and to such other persons as the court in its discretion may allow.

3/22/05 Signed by Governor, Chapter 500
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

2005 STATE LEGISLATIVE ENACTMENTS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, COMPUTER CRIMES, IDENTITY THEFT, AND OTHER ELECTRONIC-BASED CRIMES

S.B. 1111

Requires marriage records and divorce and annulment reports to include the age and race of the parties. Divorce and annulment reports must also contain the number of minor children involved. Requires the State Registrar of Vital Records to compile, publish, and make available to the public aggregate data on the number of marriages, divorces, and annulments that occur each year in the Commonwealth from 2000 forward. The data shall be organized according to the locality in which the marriage license is issued or in which the divorce or annulment report is certified, and shall include but not be limited to information regarding age and race of the parties. The data on divorce and annulments shall also include information regarding the number of minor children involved. The State Registrar is required to post, update, and maintain this information on the Department of Health website. Names, addresses, Social Security numbers, and any other personal identification information shall not be included. This is a recommendation from the Virginia Commission on Youth.

3/23/05 Signed by Governor, Chapter 679
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

S.B. 1147

Computer crimes; phishing; penalty. Makes it a Class 6 felony to fraudulently obtain, record, or access from a computer the following identifying information of another: (i) social security number; (ii) driver's license number; (iii) bank account numbers; (iv) credit or debit card numbers; (v) personal identification numbers (PIN); (vi) electronic identification codes; (vii) automated or electronic signatures; (viii) biometric data; (ix) fingerprints; (x) passwords; or (xi) 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. Any person who sells or distributes such information or uses it to commit another crime is guilty of a Class 5 felony.

03/26/05 Signed by Governor, Chapter 760
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

S.B. 1163

Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 joint study on Computer Crimes by the Joint Commission on Technology and Science and Virginia State Crime Commission. Modernizes definitions of "computer", "using a computer" and "without authority" to comport with changing technology. Revises provisions regarding computer trespass, a Class 1 misdemeanor, unless the damage to the property of another is $1,000 ($2,500 under current law) or more, in which case it is a Class 6 felony. Provisions regarding computer invasion of privacy are rewritten to include unauthorized gathering of identifying information and Class 6 penalties added for persons with previous convictions, selling or distributing the information to another or using the information in the commission of another crime. Adds as a new Class 6 felony using a computer to fraudulently gather identifying information of another (phishing), unless the information is sold or distributed to another or the information is used in the commission of another crime, in which case it is a Class 5 felony. Statute of limitation and venue provisions are relocated in the Code.

3/26/05 Signed by Governor, Chapter 761
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

WASHINGTON

H.B. 1012

Prohibits an unauthorized person or entity from installing software on a consumer's computer that would take over control of the computer, modify its security settings, collect the user's personally identifiable information, interfere with its own removal, or otherwise deceive the authorized user.

05/17/05 Signed by Governor, Chapter 500
National Conference of State Legislatures
2005 Enacted State Legislation Relating to Spyware or Adware (current through 10/25/2005)

H.B. 1385

Provides that when any instrument, except those generated by governmental agencies, is presented to a county auditor or recording officer for recording, the document may not contain the following information: (1) A Social Security number; (2) a date of birth identified with a particular person; or (3) the maiden name of a person's parent so as to be identified with a particular person.

4/22/05 Signed by Governor, Chapter 134
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1694

Revises provisions for the protection of public employee personal information, including Social Security numbers.

Signed by Governor 5/4/05, Chapter 284
National Conference of State Legislatures
Enacted Social Security Numbers Legislation - 2005 Session (current through 10/25/2005)

H.B. 1888

Provides that no person may solicit, request, or take any action to induce another person to provide personally identifying information by means of a web page, electronic mail message, or otherwise using the internet by representing oneself, either directly or by implication, to be a business or individual without the authority or approval of such business or individual. Provides that damages to a consumer resulting from the practices prohibited by this act are up to five hundred dollars per violation, or actual damages, whichever is greater.

5/10/05 Signed by Governor, Chapter 378
National Conference of State Legislatures
2005 Enacted State Legislation Relating to "Phishing" (current through 10/25/2005)

S.B. 5418

Declares that a "security freeze" means a notice placed in a consumer's credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. If a security freeze is in place, information from a consumer's credit report may be released to a third party without prior express authorization from the consumer. Does not prevent a consumer credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

5/9/05 Signed by Governor, Chapter 342
National Conference of State Legislatures
Consumer Report Security Freeze Legislation (current through 10/25/2005)

S.B. 5939

Requires police and sheriff's departments to provide a police report or original incident report at the request of any consumer claiming to be a victim of identity theft.

5/10/05 Signed by Governor, Chapter 366
National Conference of State Legislatures
2005 Enacted Identity Theft Legislation (current through 10/25/2005)

S.B. 6043

Requires any agency, person, or business that owns and licenses computerized data that includes personal information, to inform Washington consumers of any breach of their data security, following discovery or notification of the beach. The notification must be made without unreasonable delay, consistent with the needs of law enforcement. Notification may not impede a criminal investigation. "Personal information" covered by the duty to notify includes: Social Security numbers, driver's license, or ID card numbers; and credit and debit card numbers in combination with access codes. Personal information does not include publicly-available information from federal, state, and local government records. Notice of the security breach may be provided by written or electronic notice, or by a "substitute notice" by e-mail, conspicuous website posting, or major statewide media. As a matter of public policy, consumers cannot waive their right to notice. Remedies include a civil action to recover damages, or injunctive relief against a business that violates the notice requirements.

5/10/05 Signed by Governor, Chapter 368
National Conference of State Legislatures
2005 Enacted Financial Privacy Legislation (current through 10/25/2005)

WYOMING

H.B. 205

Defines unlawful skimming and establishes it as a felony.

Signed by governor 3/12/05. Ch. 166. Effective March 2, 2005.
Compilation of legislation enacted in 2005 provided to the Task Force by Marvin Dang (current through 10/25/2005)

APPENDIX III

HAWAII STATUTES RELATING TO THE USE OF PERSONAL INFORMATION

Arrests

§184-5.1 **Arrest Citations** Provides for the issuance of a citation for violations, other than for those violations for which immediate arrest is authorized. The citation form shall take the name, address, social security number and other pertinent information of the person and shall issue to the person a summons and citation, printed in the form hereinafter described, mandating the person to appear and answer to the charge at a certain place and time within seven days after the arrest.

§803-6 **Arrest Citations** When making an arrest for which a warrant is not required, a police officer may issue a citation in lieu of removing the person to the police station. The citation must include the following identifying information: the name and current address of the offender, his or her social security number, and a description of the offender.

Background and Identity Checks

§281-53.5 **Liquor Licenses** Applicants for liquor licenses are required to disclose information about any criminal history. For verification purposes, the applicant shall provide the Hawaii Criminal Justice Data Center with personal identifying information that shall include, but not be limited to, the applicant's name, social security number, date of birth, and gender. This information shall be secured only for the purpose of conducting the criminal history record check authorized by this section.

§421I-12 **Cooperative Housing Projects; Applicants** Applicants shall provide the Hawaii Criminal Justice Data Center with personal identifying information that includes name, social security number, date of birth, and gender. This information shall be secured only for the purpose of conducting the criminal history record check authorized by this section.

§514A-82.1 **Employees of Condominiums** Applicants for employment as a security guard or manager, or for any position that would allow the employee access to the keys of or entry into the units of a condominium project or association funds may initiate a background check on the applicant. The applicant shall provide the Hawaii criminal justice data center with personal identifying information that shall include but not be limited to the applicant's name, social security number, date of birth, and gender. This information shall be used only for the purpose of conducting the criminal history record check authorized by this section.

846-2.7(c) **Criminal History Records Check** Any applicant or State employee subject to a criminal history record check shall submit identifying information as required by the FBI, including name, date of birth, height, weight, eye color, gender, race, and place of birth.
§846-7 **Hawaii Criminal Justice Information Center** Requires rules and procedures to protect the criminal history record information under its control from unauthorized access, disclosure, or dissemination.

§846-24 **Civil Identification** The department of the attorney general shall register and issue certificates of identification to all persons in the State applying for the certificates in accordance with the requirements of this part.

§846-28 **Application for Civil Identification** The Department of the Attorney General shall require, collect, secure, make, and maintain a record of the social security number of applicants, among other required information.

§846-35 **Civil Identification Records Confidential** All information and records acquired by the department of the attorney general under this section shall be confidential. All information and records shall be maintained in an appropriate form and in an appropriate office in the custody and under the control of the department, which shall at all times be kept separate from any similar records relating to the identification of criminals.

Child Support

§231-57.5 **Notification of Address and Social Security Number of Debtor Parent.** DAGS shall notify the CSEA of the address and social security number of each debtor who has been subject to a setoff because of a child support debt.

§571-52.6 **Child Support Order, Judgment, or Decree** Each order, judgment, or decree under chapters 571, 576B, 580, or 584 ordering a person to pay child support shall include the following provisions: (1) Both the obligor and the obligee are required to file with the state case registry, through the CSEA, upon entry of the child support order and to update as appropriate, information on the identity and location of the party, including social security number, residential and mailing addresses, telephone number, driver's license number if different from social security number, and name, address, and telephone number of the party's employer

§571-84.5 **Support Order, Decree, Judgment, or Acknowledgement** The social security number of any individual who is a party to a divorce decree, or subject to a support order or paternity determination, or has made an acknowledgment of paternity issued under chapters 571, 576B, 580, or 584 shall be placed in the records relating to the matter.

§576B-311 **Support Orders** A petitioner seeking to establish or modify a support order or to determine parentage in a proceeding under chapter 576B must verify the petition. Unless otherwise ordered under section 576B-312, the petition or accompanying documents must provide, so far as is known, the name, residential address, and social security numbers of the obligor and the obligee, and the name, sex, residential address, social security number, and date of birth of each child for whom support is sought.

§576B-312 **Nondisclosure of Information in Exceptional Circumstances** Upon a finding, which may be made ex parte, that the health, safety, or liberty of a party or child would be unreasonably put at risk by the disclosure of identifying information, or if an existing order so provides, a tribunal shall order that the address of the child or party or other identifying information not be disclosed in a pleading or other document filed in a proceeding under chapter 576B.

§576B-602 **Registration of Enforcement Order** Registration of a support order or income withholding order of another state requires accompanying information, including social security number of the obligor.

§576D-6 **Child Support Case Registry** The case registry is to contain records of cases involving CSEA and of support orders established or modified in the State since October 1, 1998. Such records shall use standardized data elements for both parents including, but not limited to, names, residential and mailing addresses, telephone numbers, driver's license numbers, names, addresses, and telephone number of each party's employer, social security numbers and other uniform identification numbers, dates of birth, and case identification numbers, and contain such other information as required by the United States Secretary of the Department of Health and Human Services.

§576D-10.5 **Child Support Liens** A notice of child support lien shall state the name and social security number (if available) of the obligor, the child support enforcement case number, the amount of the lien and the through date (if applicable), the accruing monthly amount, and the date on which the order or judgment regarding child support or public assistance debt was recorded with the bureau of conveyances.

§576D-12 **Protection of Child Support Records** The CSEA and its agents shall keep records that may be necessary or proper in accordance with chapter 576D. All applications and records concerning any individual or case shall be confidential.

§576D-13 **Suspension or Denial of Licenses** Upon a determination by the CSEA that a holder or applicant for a license is in child support arrearage or has failed to comply with a subpoena or warrant relating to child support or paternity proceedings, the CSEA shall serve notice on the obligor or individual of the agency's intent to certify the obligor or individual as noncompliant with an order of

support or a subpoena or warrant relating to a paternity or child support proceeding. The certification shall direct the appropriate licensing authority to deny or suspend the license, or to deny the application for renewal, reinstatement, or restoration of such license. Among other required information, the certification shall include the obligor's or individual's social security number. This section also obligates the appropriate licensing authority to require that the social security number of any applicant for a professional license, driver's license, occupational license, recreational license, or marriage license be recorded on the application for those licenses. The social security number shall be used solely for purposes of this chapter for child support enforcement and identification.

§576D-13 **National New Hire Directory** All employers in the State are required to report to the CSEA within twenty days of hire the name, address, and social security number of each new employee along with the name, federal identification number, and address of the employer.

§576E-11 **Administrative Orders** Orders entered pursuant to chapter 576E shall include, in addition to other information, identifying information for each party, including social security number, residential and mailing addresses, telephone number, driver's license number if different from the social security number, and name, address, and telephone number of the party's employer, unless there is a finding that such disclosure of information would unreasonably put at risk the health, safety, or liberty of a party or child.

Controlled Substances

§329-101 **Electronic Prescription Accountability System** Required information about prescriptions for controlled substances shall include the patient's date of birth and identification number.

§329-102 **Central Repository** The Central Repository is a data processing system that tracks controlled substances. It must be capable of producing is tracking by a patient's date of birth and identification number.

Elections and Voting

§11-6 **Petitions; Withdrawal of Signatures** Any voter, after signing a petition on behalf of a candidate, who seeks to withdraw his or her signature must provide written notice to the chief election officer before the petition is filed. Notice must include the voter's name, social security number, address, and date of birth, and must be signed by the voter with the name under which the voter is registered to vote.

§11-14.5 **Confidentiality of Voter Registration Information** If a life threatening circumstance exists, law enforcement personnel and their families, as well as other people as determined by the county clerk, may request the

county clerk to keep confidential the information relating to the residence address and telephone number contained in the affidavit of registration of that person, or any list or register prepared therefrom. A person may apply in writing to the chief election officer to keep his or her residence address and telephone number confidential if the disclosure of such information would result in an unwarranted invasion of personal privacy or expose the person or a member of the person's family to risk of bodily harm.

§11-15 **Voter Registration Application** Applicant must submit affidavit with name, social security number, date of birth, and residence, including mailing address.

§11-62 **Petition for Qualification of Political Parties** The petition for qualification of a political party shall include the name, signature, residence address, date of birth, and other information as determined by the chief election officer of currently registered voters comprising not less than one-tenth of one per cent of total registered voters in the State as of the last preceding general election.

§11-97 **Voter Information Record** A voter's full name, district/precinct designation, and voter status shall be public; but all other personal voter registration information is confidential except for election or government purposes.

§11-136 **Poll Book** A poll book shall not include the social security number of any person.

§12-3 **Candidate Nomination Paper Format** The nomination paper shall be in the form prescribed and provided by the chief election officer and shall include, among other information, the candidate's name, and residence address and space for the name, signature, social security number, residence address, and date of birth for each registered voter signing the form.

§12-4 **Candidate Nomination** Nomination form requires name, residence address, date of birth, social security number, and signature of the registered voters signing it.

§12-5 **Petition; Withdrawal of Signature** Any voter, after signing a petition, who seeks to withdraw his or her signature must provide written notice to the chief election officer before petition is filed. The notice must include the voter's name, social security number, residence address, date of birth, and signature.

§15-4 **Absentee Ballots** Registered voters may request an absentee ballot for primary and special primary elections. The request shall include information such as the person's social security number, date of birth, and the address under

which the person is registered to vote. The request shall also include the address to which the person wishes the requested ballot forwarded.

Family Law

§580-16 **Divorce Decrees; Support Orders** The social security number of any individual who is party to a divorce decree or subject to a support order issued under chapter 580 shall be placed in the records relating to the matter.

§584-3.5 **Expedited Paternity Determination** The voluntary acknowledgment of paternity form shall include the social security number of each parent. The completed form, including the social security numbers, shall be transmitted to the Department of Health, so that the birth certificate issued includes the name of the legal father of the child, which shall be promptly recorded by the department of health.

§584-23.5 **Determination of Paternity** The social security number of any individual who is subject to a paternity judgment or acknowledgment, or support order issued under chapter 584 shall be placed in the records relating to the matter.

Human Services

§346-10 **Department of Human Services Records** All applications and records concerning any applicant or recipient shall be confidential.

§346-11 **Department of Human Services Records** Provides penalties for the unauthorized disclosure of confidential applications or records, or knowingly aiding and abetting the inspection of applications or records by an unauthorized person.

§346-153 **Child Care Facility** Records of deficiencies and complaints are available for public inspection, however with respect to records of family child care homes and group child care homes, sensitive personal information or information provided to DHS with the understanding that it would not be publicly divulged shall be deleted or obliterated prior to making the records available to the public.

§346-45 **Adult Protective Proceedings** The court shall maintain records of all adult protective proceedings under chapter 346. Such records may be inspected only by the dependent adult, and his or her guardian, conservator, their respective attorneys, the guardian ad litem of the dependent adult, and the other parties and their respective attorneys or guardians ad litem. All other requests for information contained in the confidential record shall be made in writing and shall include the reasons for the request and how the information is to be used and may be granted by the court for good cause.

Licenses and Permits

§134-2 **Firearm Permits** Prior to acquiring ownership or possession of a firearm, a person is required to obtain a permit. The permit application form shall include the applicant's name, address, sex, height, weight, date of birth, place of birth, social security number, and information regarding the applicant's mental health history and shall require the fingerprinting and photographing of the applicant by the police department of the county of registration.

§286-102.5 **Selective Service Registration** Department of Motor Vehicles to collect personal information from applicants for instruction permits or driver's licenses who are required to register with the Selective Service System.

§286-109 **Driver's Licenses** The examiner of drivers shall not issue or renew any driver's license using the driver's social security number on the driver's license.

§286-111 **Driver's Licenses** An application for a driver's license shall state the full name, date of birth, sex, occupation, social security number (if the applicant is eligible for a social security number), the residence address and business address, if any, of the applicant.

§286-238 **Commercial Driver's Licenses** An application for a commercial driver's license shall include the full name, date of birth, a physical description including sex and height, social security number, the business and residence addresses, and a photograph of the applicant, along with any required certifications.

§286-239 **Commercial Driver's Licenses** A commercial driver's license number shall not be the licensee's social security number.

§302A-807 **Licensing of Teachers** Upon the revocation of a teacher's license, the board of education may disclose the name, date of birth, social security number, and other pertinent information about the former licensee to the department of education and other national teacher certification agencies.

§436B-10 **Professional and Vocational Licenses** Applicants for professional and vocational licenses shall provide legal name, current residence, business and mailing addresses, telephone number, current phone numbers; an affirmation that they are beyond the age of majority, criminal history, if any, and social security number, if federal law authorizes its disclosure.

§431:3A-101 **Insurance Licensees; Treatment of Nonpublic Personal Information** This section governs the treatment of nonpublic personal financial

information about individuals by all insurance licensees. It requires notice about a licensee's privacy policy, conditions of disclosure, and opt out options.

§431:3A-303 **Insurance Licensees; Limits on Sharing Account Number Information for Marketing Purposes** A licensee shall not disclose, directly or through an affiliate other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. A licensee shall not disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

§463-9 **Private Investigators License** The information required on an application for a license includes a statement of the applicant's full name, age, date and place of birth, and residence and business addresses.

Merchants and Dealers

§445-134.11 **Pawn Transaction Agreements** All pawnbroker transaction agreements shall include the following identifying information: the name, address, and telephone number of the pawnbroker, the name, address, date of birth, and telephone number of the customer, and the type of identification presented by the customer.

§486M-2 **Pawnbrokers and Secondhand Dealers** Required records of every transaction must include the name, address, and telephone number of the dealer, the name, address, date of birth, age, signature of the customer, and the number from the photo identification presented by the customer.

§487D-2 **Retail Merchant Club Cards** Merchant club card issuers may not require social security numbers on applications, except optional credit card applications, and are prohibited from sharing personal information with unaffiliated third parties.

Other Records

§235-7.5 **Certain Unearned Income of Minor Children Taxed as if Parent's Income** In instances when this section applies, the child's tax return shall include his or her parent's social security number.

§237-3.5 **Rental Collection Agreements** Every written rental collection agreement shall have on the first page of the agreement the name, address, social security number, and, if available, the general excise tax number of the

owner of the real property being rented, the address of the property being rented, and a statement regarding the requirement to pay General Excise Tax.

§256-4 **College Savings Program** Application for a college savings program account requires the name, address, and social security number or employer identification number of the account owner.

§286-47 **Vehicle Registration Certificate** Requires that the certificate of registration for all motor vehicles be kept within the vehicle.

§286-172 **Vehicle Registration Records** Authorizes the release of vehicle registration information pursuant to rules adopted by the Director of Transportation, or to anyone required or authorized by law to give written notice by mail to owners of vehicles. Vehicle registration information may also be released to any person having a legitimate reason, however, this requires an affidavit stating the reasons for obtaining the information and making assurances that the information will be used only for such reasons, that individual identities will be properly protected, and that the information will not be used to compile a list of individuals for the purposes of any commercial solicitation by mail or otherwise, or the collection of delinquent accounts or any other purpose not allowed or provided for by the rules.

Professional Fundraisers

§467B-12 **Filing Requirements for Professional Fundraising Counsel and Professional Solicitors** Every professional fund-raising counsel or professional solicitor, prior to any solicitation, shall file a statement with the DCCA. The written statement shall list the names, addresses, and social security numbers of all officers, agents, servants, employees, directors, and independent contractors of a professional fund-raising counsel, and the names, addresses, and social security numbers of all officers, agents, servants, employees, directors, and independent contractors of a professional solicitor.

Public Records

§92F-12 **Disclosure Required** Lists information that agencies are required to make available for public inspection and disclosure. Specifies that social security numbers are to be redacted before disclosure of payroll records for public works contracts.

§92F-14 **Personal Information; Significant Privacy Interest** Enumerates information in which a person has a significant privacy interest. Establishes a standard to determine whether disclosure of a government record is an invasion of personal privacy.

§231-19.5 **Disclosure of Written Tax Opinions** Written opinions shall be open to public inspection and copying as provided in this section, notwithstanding sections 235-116, 236D-15, 237-34, and 237D-13 and any other law restricting disclosure of tax returns or tax return information to the contrary. Before making a written opinion available for public inspection and copying, the Department of Taxation shall segregate from the opinion trade secrets or other confidential, commercial, and financial information, and identifying details such as the name, address, and social security or tax identification number of the person to whom the written opinion pertains and of any other person identified in the written opinion. Segregated text shall not be disclosed under this section.

State Employees

§40-54 **Payroll Deductions** Authorizes the Comptroller to make payroll deductions for specific purposes.

§40-54.5 **Payroll Deductions** Requires disclosure for administrative purposes of the name, social security number, and amounts and dates of voluntary and mandatory payroll deductions to the recipient of funds from such deductions.

§88-44 **Enrollment in Employees' Retirement System** In addition to whatever other information the board of trustees may require, an employee becoming a member of ERS shall present evidence of his or her date of birth.

§88-103.5 **Employees' Retirement System** ERS shall disclose to the Hawaii employer-union health benefits trust fund and employee organizations information related to the administration of pension, annuity, or retirement allowance deductions, as follows: name, social security number, and amounts and dates of both voluntary and mandatory deductions remitted to the recipient.

Subpoenas and Judgments

§453-17 **Subpoena of Peer Review Adverse Decision Report** The DCCA may subpoena medical records of patients whose cases were reviewed by a peer review committee. Before production, a medical society, hospital, or health care facility shall expunge from the documents only the following patient identifiers: name, address, telephone number, hospital identification number, and social security number.

§501-151 **Pending Actions; Judgments** All judgments affecting the title to real property must include the social security number, general excise taxpayer identification number, or federal identification number for persons, corporations, partnerships or other entities against whom the judgment is rendered.

§502-033 **Judgments; Bureau of Conveyances** Except as otherwise provided, every judgment recorded by the bureau of conveyances shall contain

or have endorsed on it the social security number, general excise taxpayer identification number, or federal employer identification number for persons, corporations, partnerships, or other entities against whom a judgment is rendered.

§504-1 **Registration of Federal Judgments** Judgments of federal courts may be registered, recorded, docketed, and indexed in the bureau of conveyances or with the assistant registrar of the land court in the same manner as judgments of the courts of the State. Except as otherwise provided, every judgment shall contain or have endorsed on it the social security number, general excise taxpayer identification number, or federal employer identification number for persons, corporations, partnerships, or other entities against whom the judgment is rendered.

§612-11 **Master Jury List** Each year the clerk for each circuit shall compile a master list that shall consist of all voter registration lists for the circuit. The list shall be supplemented with names from other lists of persons resident in the circuit, such as lists of taxpayers and drivers' licenses. This includes names, addresses, and social security numbers taken from income tax returns and estimates notwithstanding section 235-116 (confidentiality of tax returns).

§612-15 **Certified Jury Lists** Requires annual compilation of certified grand jury and jury lists for each circuit from names on the jury wheel.

§636-3 **Judgments** Except as otherwise provided, every judgment shall contain or have endorsed on it the social security number, State of Hawaii general excise taxpayer identification number, or federal employer identification number for persons, corporations, partnerships, or other entities against whom the judgment is rendered.

Vital Statistics Records

§338-7 **Registration of Foundlings** Requires completion of a Department of Health form that includes the date and place of finding or assumption of custody of the foundling, the sex, color or race, approximate age of the child, name given to the child. The date of birth shall be determined by approximation. The registration form shall constitute certificate of birth. In the event that the child is identified and a regular certificate of birth is found or obtained, the foundling report shall be sealed and filed and may be opened only upon order by a court of competent jurisdiction.

§338-11 **Vital Statistics** Birth and death certificates must include, at a minimum, information required by the Public Health Service, National Center for Health Statistics. Death certificates must include the deceased's social security number.

§572-6 **Marriage Licenses** Applicants for a marriage license shall file a written application. The application shall be accompanied by a statement signed and sworn to by each of the persons, setting forth: the person's full name, date of birth, social security number, residence; their relationship, if any; the full names of parents; and that all prior marriages, if any, have been dissolved by death or dissolution. If all prior marriages have been dissolved by death or dissolution, the statement shall also set forth the date of death of the last prior spouse or the date and jurisdiction in which the last decree of dissolution was entered. Any other information consistent with the standard marriage certificate as recommended by the Public Health Service, National Center for Health Statistics, may be requested for statistical or other purposes, subject to approval of and modification by the department of health; provided that the information shall be provided at the option of the applicant and no applicant shall be denied a license for failure to provide the information.

JUSTIFICATION SHEET

DATE: DECEMBER 21, 2005

DEPARTMENT: Attorney General

TITLE: A BILL FOR AN ACT RELATING TO IDENTITY THEFT.

PURPOSE: To include in the offense of identity theft in the third degree the unauthorized possession of confidential personal information; add a new definition of "confidential personal information"; and add identity theft in the first degree, identity theft in the second degree and identity theft in the third degree to the list of repeatable offenses for purpose of enhanced sentencing.

MEANS: Amend sections 706-606.5(1), 708-800, and 708-839.8, Hawaii Revised Statutes.

JUSTIFICATION: Identity theft is a growing problem in the State of Hawaii. The unauthorized possession of confidential personal information is the precursor to the crime of identify theft because perpetrators will use confidential personal information to carry out the theft. Law enforcement agencies routinely find law violators in possession of confidential personal information of others in the form of mail, identification cards or receipts. However, current laws fail to adequately address this violation as violators are either released or charged with a petty misdemeanor theft. To provide law enforcement with the tools to better combat identity theft, the act of possessing "confidential personal information" without proper authorization should be made a criminal offense and the crime of identity theft should be amended as a repeatable offense warranting harsher criminal penalties.

GENERAL FUND: None.

APPENDIX IV

OTHER FUNDS:	None.
PPBS PROGRAM DESIGNATION:	None.
OTHER AFFECTED AGENCIES:	Judiciary, county police, county prosecutors, and the Office of the Public Defender.
EFFECTIVE DATE:	Upon approval.

APPENDIX IV

__.B. NO._____

A BILL FOR AN ACT

RELATING TO IDENTITY THEFT.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Section 706-606.5, Hawaii Revised Statutes, is amended by amending subsection (1) to read as follows:

"(1) Notwithstanding section 706-669 and any other law to the contrary, any person convicted of murder in the second degree, any class A felony, any class B felony, or any of the following class C felonies: section 188-23 relating to possession or use of explosives, electrofishing devices, and poisonous substances in state waters; section 707-703 relating to negligent homicide in the first degree; section 707-711 relating to assault in the second degree; section 707-713 relating to reckless endangering in the first degree; section 707-716 relating to terroristic threatening in the first degree; section 707-721 relating to unlawful imprisonment in the first degree; section 707-732 relating to sexual assault or rape in the third degree; section 707-735 relating to sodomy in the third degree; section 707-736 relating to sexual abuse in the first degree; section 707-751 relating to promoting child abuse in the second degree; section 707-766 relating to extortion in the second

degree; section 708-811 relating to burglary in the second degree; section 708-821 relating to criminal property damage in the second degree; section 708-831 relating to theft in the first degree as amended by Act 68, Session Laws of Hawaii 1981; section 708-831 relating to theft in the second degree; section 708-835.5 relating to theft of livestock; section 708-836 relating to unauthorized control of propelled vehicle; section 708-839.6 relating to identity theft in the first degree; section 708-839.7 relating to identity theft in the second degree; section 708-839.8 relating to identity theft in the third degree; section 708-852 relating to forgery in the second degree; section 708-854 relating to criminal possession of a forgery device; section 708-875 relating to trademark counterfeiting; section 710-1071 relating to intimidating a witness; section 711-1103 relating to riot; section 712-1203 relating to promoting prostitution in the second degree; section 712-1221 relating to gambling in the first degree; section 712-1224 relating to possession of gambling records in the first degree; section 712-1243 relating to promoting a dangerous drug in the third degree; section 712-1247 relating to promoting a detrimental drug in the first degree; section 134-7 relating to ownership or possession of firearms or ammunition by persons convicted of certain crimes; section 134-8

relating to ownership, etc., of prohibited weapons; section 134-9 relating to permits to carry, or who is convicted of attempting to commit murder in the second degree, any class A felony, any class B felony, or any of the class C felony offenses enumerated above and who has a prior conviction or prior convictions for the following felonies, including an attempt to commit the same: murder, murder in the first or second degree, a class A felony, a class B felony, any of the class C felony offenses enumerated above, or any felony conviction of another jurisdiction shall be sentenced to a mandatory minimum period of imprisonment without possibility of parole during such period as follows:

(a) One prior felony conviction:

(i) Where the instant conviction is for murder in the second degree or attempted murder in the second degree--ten years;

(ii) Where the instant conviction is for a class A felony--six years, eight months;

(iii) Where the instant conviction is for a class B felony--three years, four months;

(iv) Where the instant conviction is for a class C felony offense enumerated above--one year, eight months;

(b) Two prior felony convictions:

(i) Where the instant conviction is for murder in the second degree or attempted murder in the second degree--twenty years;

(ii) Where the instant conviction is for a class A felony--thirteen years, four months;

(iii) Where the instant conviction is for a class B felony--six years, eight months;

(iv) Where the instant conviction is for a class C felony offense enumerated above--three years, four months;

(c) Three or more prior felony convictions:

(i) Where the instant conviction is for murder in the second degree or attempted murder in the second degree--thirty years;

(ii) Where the instant conviction is for a class A felony--twenty years;

(iii) Where the instant conviction is for a class B felony--ten years;

(iv) Where the instant conviction is for a class C felony offense enumerated above--five years."

SECTION 2. Section 708-800, Hawaii Revised Statutes, is amended by adding a new definition to read as follows:

""Confidential personal information" means information associated with an actual person or a fictitious person that is a driver's license number, a social security number, a state identification number, an employee identification number, a mother's maiden name, an identifying number of a depository account, a bank account number, a password, or a personal identification number (PIN) or code used for accessing loan, credit, or banking information."

SECTION 3. Section 708-839.8, Hawaii Revised Statutes, is amended to read as follows:

"[~~[~~]§**708-839.8**[~~]~~] **Identity theft in the third degree.** (1) A person commits the offense of identity theft in the third degree if that person [~~makes~~]:

(a) Makes or causes to be made, either directly or indirectly, a transmission of any personal information of another by any oral statement, any written statement, or any statement conveyed by any electronic means, with the intent to commit the offense of theft in the third or fourth degree from any person or entity[~~.~~]; or

(b) Intentionally or knowingly possesses, without authorization, any confidential personal information of another in any form, including, but not limited to, mail, physical documents, identification cards, or information stored in digital form.

(2) It is an affirmative defense that the person who possessed the confidential personal information of another did so under the reasonable belief that the person was authorized to possess the confidential personal information of another by the other person.

[~~(2)~~] (3) Identity theft in the third degree is a class C felony."

SECTION 4. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 5. This Act shall take effect upon its approval.

INTRODUCED BY:_____

Report Title:
State Identity Theft Task Force

Description:
Changes name of task force, expands its responsibilities, and extends its life until 6/30/07. Adds the chief justice or designee, and representatives from each county police department, the prosecutor's office, and the U.S. Postal Service to the task force membership.

Appendix IV

THE SENATE
TWENTY-THIRD LEGISLATURE, 2006
STATE OF HAWAII

S.B. NO.

A BILL FOR AN ACT

RELATING TO ELECTRONIC COMMERCE.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Act 65, Session Laws of Hawaii 2005, is amended by amending section 2 to read as follows:

"SECTION 2. (a) There is established [~~within the department of the attorney general~~] a [~~Hawaii anti-phishing~~] state identity theft task force to examine options to prevent electronic commerce-based crimes in the State[~~.~~] and to safeguard and protect from identity theft all personal identifying information collected by the State.

(b) The [~~Hawaii anti-phishing~~] state identity theft task force shall include members as follows:

(1) The attorney general or the attorney general's designee;

(2) The director of the office of consumer protection;

(3) The United States Attorney for the District of Hawaii or the United States Attorney's designee;

(4) Two members of the Hawaii state senate appointed by the president of the senate;

(5) Two members of the Hawaii state house of representatives appointed by the speaker of the house of representatives;

(6) Two members representing the financial services industry, one appointed by the president of the senate and one appointed by the speaker of the house of representatives;

(7) A member of the Honolulu police department's criminal investigation division; [~~and~~]

(8) A member of the Honolulu field office's United States Secret Service electronic crimes unit[~~.~~];

(9) The chief justice of the supreme court or the chief justice's designee;

(10) A member representing each of the county police departments appointed by the respective police chiefs;

(11) The prosecuting attorney for the city and county of Honolulu, or the prosecuting attorney's designee; and

(12) A member representing the United States Postal Service.

(c) The task force shall:

(1) Examine the policies, procedures, and operations of state agencies charged with the responsibility of

developing policies to prevent electronic commerce-based crimes, monitoring electronic commerce-based criminal activity, and enforcing electronic commerce-based criminal sanctions;

(2) Review other jurisdictions' activities, policies, directives, and laws related to preventing electronic commerce-based crimes and derive best practices models therefrom;

(3) Explore any other options available to the task force to deter electronic commerce-based crimes from occurring in the State; [~~and~~]

(4) Establish findings and develop recommendations on how the State may best deter electronic commerce-based crimes from occurring in the State[~~.~~]; and

(5) Identify best practices to prevent identity theft by reviewing other jurisdictions' activities, policies, and laws related to protecting personal identifying information collected by the State, and establish a timetable for the immediate removal of personal identifying information from public records.

(d) The task force shall submit its findings and recommendations to the legislature, including any proposed

legislation, no later than twenty days prior to the convening of the [~~2006~~] 2007 regular session.

(e) The [~~department of the attorney general~~] senate majority office and the house majority staff office shall provide the research and logistical support services necessary to assist the task force in achieving its purpose as required under this Act.

(f) The task force shall cease to exist on June 30, [~~2006~~] 2007."

SECTION 2. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 3. This Act shall take effect on June 29, 2006.

INTRODUCED BY: _____