Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

UNITED STATES LEGISLATION RELEVANT TO IDENTITY THEFT:

AN ANNOTATED REVIEW

March, 2007

CIPPIC Working Paper No. 3B (ID Theft Series)

www.cippic.ca

CIPPIC Identity Theft Working Paper Series

This series of working papers, researched in 2006, is designed to provide relevant and useful information to public and private sector organizations struggling with the growing problem of identity theft and fraud. It is funded by a grant from the Ontario Research Network on Electronic Commerce (ORNEC), a consortium of private sector organizations, government agencies, and academic institutions. These working papers are part of a broader ORNEC research project on identity theft, involving researchers from multiple disciplines and four post-secondary institutions. For more information on the ORNEC project, see www.ornec.ca .

Senior Researcher: Wendy Parkes
Research Assistant: Thomas Legault
Project Director: Philippa Lawson

Suggested Citation:

CIPPIC (2007), "United States Legislation Relevant to Identity Theft: Annotated Review", CIPPIC Working Paper No.3B (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Working Paper Series:

No.1: Identity Theft: Introduction and Background
No.2: Techniques of Identity Theft
No.3: Legislative Approaches to Identity Theft: An Overview
No.3A: Canadian Legislation Relevant to Identity Theft: Annotated Review
No.3B: United States Legislation Relevant to Identity Theft: Annotated Review
No.3C: Australian, French, and U.K. Legislation Relevant to Identity Theft: Annotated Review
No.4: Caselaw on Identity Theft
No.5: Enforcement of Identity Theft Laws
No.6: Policy Approaches to Identity Theft
No.7: Identity Theft: Bibliography

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established at the Faculty of Law, University of Ottawa, in 2003. CIPPIC's mission is to fill voids in law and public policy formation on issues arising from the use of new technologies. The clinic provides undergraduate and graduate law students with a hands-on educational experience in public interest research and advocacy, while fulfilling its mission of contributing effectively to the development of law and policy on emerging issues.

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

TABLE OF CONTENTS

Page

1. ANNOTATED REVIEW

1.1. Federal Legislation

There are a multitude of U.S. federal laws targeting different aspects of identity crimes. These laws can be divided into four categories: identity theft specific laws, false identification laws, privacy and personal data laws, and credit laws. There are also other "general" statutes that are applicable to identity theft.

1.1.1. Identity Theft Specific Laws

1.1.1.1. Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C § 10281

The *Identity Theft and Assumption Deterrence Act of 1998* was the first piece of federal legislation to deal directly with identity theft. This Act introduced a new offence for when an individual "(7) knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law;"

It also defines "means of identification" as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

> "(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
> (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
> (C) unique electronic identification number, address, or routing code; or
> (D) telecommunication identifying information or access device (as defined in section 1029(e));…"

Finally, the Act established the Federal Trade Commission (FTC) as the government entity charged with establishing "procedures to ... log and acknowledge the receipt of complaints by individuals", as well as educating and assisting potential victims.

1.1.1.2. Identity Theft Penalty Enhancement Act, 18 U.S.C § 10012

This Act establishes penalties for aggravated identity theft. Aggravated identity theft is committed when an individual "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" while committing or in relation to the

---

[1] *Identity Theft and Assumption Deterrence Act*, 18 U.S.C § 1028, online: <http://www.ftc.gov/os/statutes/itada/itadact.htm>.

[2] *Identity Theft Penalty Enhancement Act*, 18 U.S.C § 1001, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

commission of another felony. Aggravated identity theft is also committed if the related felony is a terrorism felony.

This statute also requires that sentencing guidelines for "offences in which the defendant exceeds or abuses the authority of his or her position in order to obtain unlawfully or use without authority any means of identification" be reviewed to appropriately punish identity theft committed by insiders.

1.1.1.3. Fair and Accurate Credit Transactions Act (FACTA), U.S.C. § 16813

When consumers contest information in their credit report, this Act imposes a duty on credit bureaus to indicate that fact in credit reports which contain the disputed information.

This Act also limits the credit card information which can be printed on receipts given to the consumer at the point of sale. Only the last five digits or the expiration date can be electronically printed on receipts. This provision does not apply to "manual" paper transactions.

This Act imposes a duty on credit bureaus to notify credit report requestors of significant discrepancies between the consumer address in the request and the consumer address in the credit bureau's file.

This Act also imposes a duty on credit bureaus to place a "fraud alert" on the consumer's file when a consumer asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft. Under these circumstances, the fraud alert must remain for 90 days. The duty also requires the credit bureau to notify the other credit bureaus. When placing a "fraud alert" on a consumer file, the credit bureau must notify the consumer that he or she may request a free copy of their file.

This Act also imposes a duty to place an extended "fraud alert" on a consumer file when a consumer submits an identity theft report. To invoke this provision, a victim must have a police report. An extended fraud alert can remain up to seven years on a consumer's file. It also prohibits credit bureaus from providing the consumer's information in lists of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance. A notice of the extended "fraud alert" must also be provided to the other credit reporting agencies. A consumer who gets an extended "fraud alert" placed on his or her file can get two free copies of his or her file in the following twelve months.

When credit grantor (user) receives a credit report containing a "fraud alert", it must not extend new credit unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

---

[3] *Fair and Accurate Credit Transactions Act* (FACTA), U.S.C. § 1681, online: <http://www.ftc.gov/os/statutes/031224fcra.pdf.>

This Act also prohibits credit reporting agencies from including any information in credit reports which the consumer has identified as the consequences of identity theft. To obtain information removed, the consumer must provide a copy of an identity theft report obtained from local law enforcement agencies.

A duty is imposed on consumer reporting agencies to make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will be used for something other than a permitted purpose.

This Act makes it an offence to knowingly and wilfully obtain information about a consumer from a consumer reporting agency under false pretences and makes it an offence for an employee of a credit reporting agency to knowingly and wilfully provide information to a person not authorized to receive it.

Consumer reporting agencies must provide to an individual his or her credit report free of charge, at least once in every 12 month period. Business entities that have provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with a person who has allegedly made unauthorized use of the means of identification of the victim, must provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to the victim or to a law enforcement agency specified by the victim.

This Act also requires that any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose, properly dispose of any such information or compilation. The requirement for the proper disposal of records is implemented in the FTC Rule *Disposal of Consumer Report Information and Records*, 16 CFR Part 682.[4]

1.1.2. False Identification Laws

1.1.2.1. Fraud and related activity in connection with identification documents, 18 U.S.C. § 10285

This section of the United States Code criminalizes:

- the creation of identification document without lawful authority, the creation of false identification documents and the transfer of such documents;

[4] Federal Trade Commission, *Disposal of Consumer Report Information and Records*, 16 CFR Part 682, online: <http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf>.

[5] *Fraud and related activity in connection with identification documents*, 18 U.S.C. § 1028: online <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

- the possession with intent to use unlawfully or transfer unlawfully five or more identification documents;
- the possession of an identification document or false identification document with the intent of defrauding the United States;
- the production, transfer or possession of a document-making implement that will used to make either false identification documents or other document-making implements;
- possession of an identification document that is stolen or produced without lawful authorization with the knowledge that it was stolen or produced without lawful authorization;

1.1.2.2. Internet False Identification Act of 2000, 18 U.S.C § 10216

This Act essentially expands the existing provisions of the *Fraud and related activity in connection with identification documents, 18 U.S.C. § 1028* Act, to criminalize the electronic transfer and creation of identification documents. It also criminalizes the production of novelty identification documents.

1.1.3. Privacy and Personal Data Laws

1.1.3.1. Privacy Act of 1971, 5 U.S.C. § 552a7

This Act limits disclosure of personal information to situations where the individual has given prior consent in writing. It also imposes a duty to keep an accurate accounting of all disclosures. The collection of information is limited to what is relevant and necessary to accomplish a purpose of the agency that is required to be accomplished by statute or by Executive Order of the President.

The Act also imposes a duty on agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity

1.1.3.2. Drivers Privacy Protection Act of 1994, 18 U.S.C § 27218

This Act provides a definition of personal information, as follows: "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. It also defines highly

---

[6] *Internet False Identification Act of 2000*, 18 U.S.C § 1021, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ578.106.pdf>.

[7] *Privacy Act of 1971*, 5 U.S.C. § 552a, online: <http://www.uscg.mil/ccs/cit/cim/foia/PRIVACY_ACT_OF_1974.pdf>.

[8] *Drivers Privacy Protection Act of 1994*, 18 U.S.C § 2721, online: <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html>.

restricted personal information: "highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information.

This law restricts how personal information from state Departments of Motor Vehicles can be used. It also restricts the resale and redisclosure of personal information.

1.1.3.3. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C § 2019

This Act defines "individually identifiable health information" as any information, including demographic information, collected from an individual, that is created or received by a health care provider and relates to the physical or mental health of an individual or the provision of health services to him or her; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identity the individual.

This Act creates an offence for an individual who knowingly and wilfully executes, or attempts to execute, a scheme or artifice (1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretences, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program.

The Act creates an offence for an individual who, in any matter involving a health care benefit program, knowingly and wilfully falsifies, conceals, or covers up by any trick, scheme or makes any materially false, fictitious, or fraudulent statements or representations or documents in connection with the delivery of or payment for health care benefits, items, or services.

A duty is imposed on the Health and Human Services Secretary to adopt standards for transactions and data elements for such transactions, to enable health information to be exchanged electronically. This duty includes adoption of standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system.

The Secretary must also adopt security standards to protect electronic health information. These standards must take into account the technical capabilities of the record systems, the cost of security measures, the need for training and the value of computerized audit trails.

A similar duty is imposed on persons who maintain or transmit health information. They shall maintain reasonable and appropriate administrative, technical, and physical safeguards to (a) ensure the integrity and confidentiality of the information and (b) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information.

---

[9] *Health Insurance Portability and Accountability Act of 1996* (HIPAA), 42 U.S.C § 201, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ191.104.pdf>.

This Act creates offences for an individual who knowingly and in violation of this part (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person.

The Health and Human Services Secretary is mandated to make recommendations to address (1) The rights that an individual who is a subject of individually identifiable health information should have; (2) The procedures that should be established for the exercise of such rights; and (3) The uses and disclosures of such information that should be authorized or required.

1.1.3.4. Gramm-Leach-Bliley Act, 12 U.S.C § 181110

This Act is also known as the *Financial Services Modernization Act of 1999* (FSMA).

Section 501 imposes a duty on financial institutions to respect the appropriate standards relating to administrative, technical, and physical safeguards: 1) to ensure the security and confidentiality of customer records and information; 2) to protect against any anticipated threats or hazards to the security or integrity of such records; and 3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Section 502 limits the disclosure of consumer information to third parties to situations where the consumer has received a notice of such disclosure. The notice, in writing, must disclose that such information may be disclosed to such third parties. Financial institutions must also provide an opportunity for the consumer to opt-out of the disclosure before any disclosure takes place. Section 502 also prohibits the disclosure of account numbers to third parties other than to a consumer reporting agency.

Section 503 imposes a duty on financial institutions to provide their privacy policy to consumers when establishing a customer relationship and at least once annually during the continuation of the relationship. Specifically, financial institutions must disclose information pertaining to the following practices in their privacy policy: (1) disclosing non-public personal information to affiliates and non-affiliated third parties, consistent with section 502, including the categories of information that may be disclosed; (2) disclosing non-public personal information of persons who have ceased to be customers of the financial institution; and (3) protecting the non-public personal information of consumers.

Section 521 makes it an offence to collect, attempt to collect, disclose or attempt to disclose customer information of a financial institution of another person by making false, fictitious, or fraudulent statements or representations, or by providing any document to an officer, employee or agent of a financial institution, knowing that the document is forged,

[10] *Gramm-Leach-Bliley Act*, 12 U.S.C § 1811: online http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf.

counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation. It also makes it an offence to ask someone to get consumer information based on the above methods.

1.1.3.5. Social Security Number Confidentiality Act of 2000, 31 U.S.C § 330111

This Act imposes an obligation on the Treasury Secretary to take such actions as are necessary to ensure that Social Security account numbers (including derivatives of such numbers) are not visible on or through unopened mailings of cheques or other drafts.

1.1.3.6. Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C § 10112

Section 902 of this Act requires the Secretary of Veterans Affairs to obtain an independent risk analysis in the case of a data breach. The analysis must be conducted by a non-Department entity or by the Office of Inspector General of the Department. The analysis must determine the level of risk of misuse of any sensitive personal information.

If a risk is found to exist, the Secretary is required to provide credit protection services in accordance with the regulations.

The Act also requires Secretary to prohibit contractors from disclosing personal information. It also requires that contractors and subcontractors notify the Secretary in the event of any data breach.

The Act also requires the Secretary to submit a report on any data breach to the Committees on Veterans' Affairs of the Senate and House of Representatives.

1.1.4. Credit Laws

1.1.4.1. Fair Credit Reporting Act, 15 U.S.C. § 168113

The purpose of this Act is to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.

The Act limits the circumstances under which a credit reporting agency may furnish a credit report about an individual. It also prohibits individuals from getting a credit report unless it is obtained for a purpose for which the consumer report is authorized to be furnished or the

---

[11] *Social Security Number Confidentiality Act of 2000*, 31 U.S.C § 3301, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ433.106.pdf>.

[12] *Veterans Benefits, Health Care, and Information Technology Act of 2006*, 38 U.S.C § 101, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s3421enr.txt.pdf>.

[13] *Fair Credit Reporting Act*, 15 U.S.C. § 1681, online: <http://www.ftc.gov/os/statutes/031224fcra.pdf>.

purpose is certified in accordance with section 607. The disclosure of medical information is also limited.

Section 619 prohibits knowingly and wilfully obtaining information about a consumer from a consumer reporting agency under false pretences. Section 620, an insider abuse provision, prohibits knowingly and willfully providing information concerning an individual from the agency's files to a person not authorized to receive that information.

This Act also mandates the creation of regulations pertaining to the proper disposal of consumer information, or any compilation of consumer information.

1.1.4.2. Electronic Funds Transfer Act, 15 U.S.C. § 169314

This Act limits a consumer's financial liability to $50 in case of unauthorized electronic fund transfers if the consumer notifies the card issuer within 60 days of receiving the statement containing the unauthorized charge. The burden of proof lies with the card issuer to show that the charge was either authorized or that it was not notified within the prescribed time.

This Act prohibits issuing any card, code, or other means of access to such consumer's account to consumers unless the consumer requests it. It also imposes civil liability on those who fail to comply with the provisions of the Act.

1.1.4.3. Fair Credit Billing Act, 15 U.S.C § 160115

This Act establishes procedures to correct billing errors on credit card accounts when the consumer reports unauthorized activity or errors within 60 days of receiving the statement containing the error or unauthorized activity.

1.1.4.4. Fair Debt Collections Practices Act, 15 U.S.C § 160116

This Act limits the behaviours and tactics that debt collectors use. Debt collectors cannot contact a debtor more than once to get his or her location information. Debt collectors, once they are aware that a debtor is represented by an attorney, must only communicate with that attorney.

Debt collectors are prohibited from communicating with a consumer: 1) at any unusual time or place or a time or place known or which should be known to be inconvenient to the consumer 2) if the debt collector knows the consumer is represented by an attorney with respect to such debt; or 3) at the consumer's place of employment if the debt collector knows or has reason to know that the consumer's employer prohibits the consumer from

[14] *Electronic Funds Transfer Act*, 15 U.S.C. § 1693, online: <http://www4.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_41_20_VI.html>.
[15] *Fair Credit Billing Act*, 15 U.S.C § 1601, online: <http://www.ftc.gov/os/statutes/fcb/fcb.pdf>.
[16] *Fair Debt Collections Practices Act*, 15 U.S.C § 1601, online: <http://www.yourcredit.com/assets/pdf/laws/federal/pubLaw/pl-fdcpa.PDF>.

receiving such communication. Debts collectors may not communicate, in connection with the collection of any debt, with any person other than a consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor or the attorney of the debt collector.

Debt collectors are also prohibited from communication with consumers once the consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication. For this provision, "consumer" includes the consumer's spouse, parent (if the consumer is a minor), guardian, executor, or administrator.

Debts collectors are prohibited from engaging in any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt. Debt collectors are further prohibited from using any false, deceptive, or misleading representation or means in connection with the collection of any debt. They are also prohibited from using unfair or unconscionable means to collect or attempt to collect any debt.

1.1.5. General Laws

1.1.5.1. Federal Trade Commission Act, 15 U.S.C. §§ 41-5817

This Act prohibits the use of unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.

Companies who make implicit or explicit promises about their security safeguards for information have been found to commit deceptive acts, which the Federal Trade Commission and the courts have defined as "a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances".[18]

1.1.6. Federal Identity Theft Bills

The federal legislature, in both Congress and the Senate, has been very active when it comes to identity theft. Many bills have been proposed though only a limited number of them have been adopted over the years (note is made of those bills that have in fact been enacted). Many of these bills contain the same provisions or very similar provisions. They are included here to demonstrate the high degree of interest and initiative amongst U.S. legislators and because some of the provisions contain proposals that are useful in framing recommendations for improvements in Canadian law.

This inventory focuses on identity-theft-specific bills. It should be noted that a number of other bills also consider the risk of identity theft. For example, many bills contain provisions

[17] *Federal Trade Commission Act*, 15 U.S.C. §§ 41-58, online: http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000041----000-.html.

[18] Federal Trade Commission, *Cybersecurity and Consumer Data: What's at Risk for the Consumer?*, (19 November 2003), online: <http://www.ftc.gov/os/2003/11/031119swindletest.htm>.

giving granting agencies the right to redact certain information before this information is made publicly available.

1.1.7. Bills introduced in 2001

Identity Theft Prevention Act of 2001 (S. 1399)

Purpose**:** To prevent identity theft, and for other purposes.

Description**:** This bill would impose a duty on credit card issuers to notify the account holder of the issuance of a new credit card if the new card is requested less than 30 days after the card issuers received a change of address notification. It also would impose a duty on credit reporting agencies to notify the credit report requestor if the address in the report is different than the address submitted to obtain the report. There would be a duty on credit reporting agencies to warn credit grantors about fraud alerts. An offence would be created for credit grantors who fail to comply with preauthorization procedures contained in a fraud alert. Finally, the bill would impose a duty on organizations which accept credit cards to truncate printed credit card numbers to only five digits.

Text**:** <http://www.securitymanagement.com/library/S1399_identity1201.pdf>.

Social Security Number Privacy and Identity Theft Prevention Act of 2001 (H.R. 2036, S. 1014)

Purpose**:** To amend the Social Security Act to enhance privacy protections for individuals, to prevent fraudulent misuse of the Social Security account number, and for other purposes.

Description**:** This bill proposes prohibiting 1) the sale of social security account numbers by government agencies and private organizations; 2) the display of social security account numbers to the general public, on government cheques and on driver's licences; 3) inmate access to social security numbers and their sale. It also calls for independent verification of birth records before issuing social security account numbers. Refusing to do business if a social security account number is not provided would be considered an unfair or deceptive act or practice. The bill would also impose new criminal penalties for misuse of social security account numbers.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h2036.pdf>.

Social Security On-line Privacy Protection Act (H.R. 91)

Purpose**:** To regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information.

Description**:** This Act would prohibit interactive computer services disclosing the social security account number or related personally identifiable information without the

individual's prior informed written consent. It would also allow individuals to revoke their consent to the disclosure.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h91.pdf>.

Protect Victims of Identity Theft Act of 2001 (H.R. 3368, S. 1723)

Purpose**:** To amend the *Fair Credit Reporting Act* with respect to the statute of limitations on actions.

Description**:** This Act would toll (temporarily stop) the limitations period during any period during which a defendant has materially and wilfully misrepresented any information required under this title to be disclosed to an individual. It would also set the beginning of the limitation period as the moment when a consumer discovered or should have discovered the fraud.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/s1723.pdf>.

ID Theft Loophole Closure Act (H.R. 2077)

Purpose**:** To amend the *Internal Revenue Code* of 1986 to provide for the disclosure to State and local law enforcement agencies of the identity of individuals claiming tax benefits improperly using social security numbers of other individuals.

Description**:** This bill would give the power to the Secretary of the Treasury to disclose the name, TIN, and mailing address of individuals who claim tax benefits under another individual's name.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h2077.pdf>.

Consumer Debit Card Protection Act (H.R. 29)

Purpose**:** To amend the *Electronic Fund Transfer Act* to safeguard consumers in connection with the utilization of certain debit cards.

Description**:** This bill would introduce photographs and other biometric data as unique identifiers for consumers. It would limit the liability of consumers to $50 for unauthorized electronic fund transfers. It would impose a duty on card issuers to either issue only cards which require the use of a code or unique identifier or to notify consumers, with a clear and conspicuous disclosure, that such a code or unique identifier is not required to use the card.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h1825.pdf>.

Identity Theft Protection Act of 2001 (H.R. 220)

Purpose**:** To amend title II of the *Social Security Act* and the Internal Revenue Code of 1986 to protect the integrity and confidentiality of Social Security account numbers issued under such title, to prohibit the establishment in the federal government of any uniform national identifying number, and to prohibit federal agencies from imposing standards for identification of individuals on other agencies or persons.

Description**:** This bill would repeal provisions authorizing certain usages of the social security account number. It would prevent the Social Security Administration from divulging the social security number of individuals to any agency or instrumentality of the federal government, to any state, political subdivision of a state, or agency or instrumentality of a state or political subdivision thereof, or to any other individual. This bill would also prohibit federal agencies from implementing the same identifying number or mandating a uniform standard for identification of an individual that is required to be used by other agencies.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h220.pdf>.

1.1.8. Bills introduced in 2002

Identity Theft Victims Assistance Act of 2002 (H.R. 5424, S. 1742)

Purpose**:** To prevent the crime of identity theft, mitigate the harm to individuals victimized by identity theft, and for other purposes.

Description**:** This bill would provide definitions for “financial information” and “victim”. It would impose a duty on “business entities” to provide, free of charge, any information about transactions which are the result of identity theft, to the victim. Business entities would not be obliged to provide any internet navigational data if the fraudulent transactions were committed online. It would also give the power to states to launch actions based their role as *parens patriae* if business entities violate this section of the United States Code. The *Fair Credit Reporting Act* (15 U.S.C. § 1681) would be amended to impose a duty on consumer reporting agencies to block information which is the result of identity theft from credit reports. It would also mandate the federal Coordinating Committee on False Identification to report to Congress on how the government can help with enforcement of identity theft laws and how it can provide information on terrorist activity that relates to identity theft.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h5424.pdf>.

Social Security Number Protection Act of 2002 (H.R. 4513)

Purpose**:** To strengthen the authority of the federal government to protect individuals from certain acts and practices in the sale and purchase of Social Security numbers and Social Security account numbers, and for other purposes.

Description**:** This bill would mandate that the Federal Trade Commission make regulations that control the sale and purchase of Social Security number or Social Security account number. It would make it an offence to sell or purchase this information in violation of the regulations promulgated by the Commission.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h4513.pdf>.

Identity Theft Penalty Enhancement Act of 2002 (H.R. 5588, S. 2541)

Purpose**:** To amend title 18, United States Code, to establish penalties for aggravated identity theft, and for other purposes.

Description**:** This bill would introduce the new felony of "aggravated identity theft" which is defined as "during and in relation to any felony knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person". Increased penalties would be provided if the felony being furthered by identity theft is a terrorism felony.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h5588.pdf>.

Consumer Privacy Protection Act of 2002 (H.R. 4678)

Purpose**:** To protect and enhance consumer privacy, and for other purposes.

Description**:** This bill would mandate that data collection organizations provide privacy notices to consumers and offer consumers the opportunity to prevent the sale or disclosure of their personal information. It would require that the Commission permit consumers to fill out the Commission-developed document entitled "Identity Theft Affidavit" and solicit organizations to accept the affidavit. This bill would also mandate that organizations take reasonable steps to verify the accuracy of a consumer's address, including confirming a consumer's change of address, by sending a confirmation of such change to the old and the new address of the consumer. The Secretary would be required to seek the harmonization of this Act with information privacy laws, regulations, or agreements; to the extent such harmonization is necessary for the advancement of transnational commerce, including electronic commerce.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h4678.pdf>.

Identity Theft Consumer Notification Act (H.R. 5474)

Purpose**:** To amend the *Gramm-Leach-Bliley Act* to further protect customers of financial institutions whose identities are stolen from the financial institution, and for other purposes.

Description**:** This bill would impose a duty on financial institutions to notify consumers if the security of any non public personal information maintained by the financial institution has been compromised in any way by an employee, or through any unauthorized entry into

the records. Financial institutions would also provide assistance to the consumer to remedy any such compromise and reimburse any loses incurred as a result of the compromise.

Text**:** <http://www.govtrack.us/data/us/bills.text/107/h5474.pdf>.

1.1.9. Bills introduced in 2003

Identity Theft Prevention Act (S. 223)

Purpose**:** To prevent identity theft, and for other purposes.

Description**:** See *Identity Theft Prevention Act* of 2001.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s223.pdf>.

Identity Theft and Financial Privacy Protection Act of 2003 (H.R. 2035)

Purpose**:** To prevent identity theft, and for other purposes.

Description**:** This bill would impose a duty on credit card issues to notify the account holder of the issuance of a new credit card if the new card is requested less than 30 days after the card issuers received a change of address notification. It would impose a duty on credit reporting agencies to notify the credit report requestor if the address in the report is different from the address submitted to get the report. Credit reporting agencies would have a duty to warn credit grantors about fraud alerts. There would be an offence for credit grantors who fail to comply with preauthorization procedures contained in a fraud alert. Finally, the bill would impose a duty on organizations that accept credit cards to truncate printed credit card numbers to only five digits.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h2035.pdf>.

Identity Theft Penalty Enhancement Act (H.R. 1731, S. 153)

Purpose**:** To amend title 18, United States Code, to establish penalties for aggravated identity theft, and for other purposes.

Description**:** See *Identity Theft Penalty Enhancement Act*, 18 U.S.C § 1001 p. 1.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h1731.pdf>.

Note**:** This bill was enacted July 15, 2004.

Identity Theft Penalty Enhancement Act (H.R. 29)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Penalty Enhancement Act* of 2002 (H.R. 5588, S. 2541).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h858.pdf>.

Identity Theft Protection and Information Blackout Act of 2003 (H.R. 2633)

Purpose**:** To establish methods for preventing identity theft and to amend the *Fair Credit Reporting Act* to protect consumers' sensitive, private health related information, and for other purposes.

Description**:** This bill would prohibit the sale of Social Security Numbers by the federal government or a state or a political subdivision thereof or trustee appointed, and by private organizations. It would also prohibit the display of social security numbers. Refusing to do business if a social security account number is not provided would be considered an unfair or deceptive act or practice. This bill would limit the sharing of personal medical information by consumer reporting agencies.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h2633.pdf>.

ID Theft Loophole Closure Act (H.R. 2774)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Loophole Closure Act* (H.R. 2077).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h2774.pdf>.

Identity Theft Consumer Notification Act (H.R. 29)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Consumer Notification Act* (H.R. 5474).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h818.pdf>.

Identify Theft Prevention Act of 2003 (H.R. 220)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Protection Act* of 2001 (H.R. 220).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h220.pdf>.

Identity Theft Notification and Credit Restoration Act of 2003 (H.R. 3233, 1633)

Purpose**:** To require financial institutions and financial service providers to notify customers of the unauthorized use of personal information, to amend the *Fair Credit Reporting Act* to require fraud alerts to be included in consumer credit files in such cases, and to provide customers with enhanced access to credit reports in such cases.

Description**:** This bill would impose a duty on financial institutions to notify consumers of unauthorized acquisition of computerized data or paper records which compromises the security, confidentiality, or integrity of personal information maintained by or on behalf of a financial institution. As part of the notification, credit reporting agencies would also be notified and they would have to place a fraud alert on affected consumer files. Consumer reporting agencies would have to include fraud alerts in credit reports. Requestors of credit reports would be aware of the fraud alert. Credit grantors would have a duty to follow the preauthorization procedures contained in fraud alerts before extending new credit.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h3233.pdf>.

Fair and Accurate Credit Transactions Act of 2003 (H.R. 2622)

Purpose**:** To amend title 18, United States Code, to establish penalties for aggravated identity theft, and for other purposes.

Description**:** See *Fair and Accurate Credit Transactions Act* (FACTA), U.S.C. § 1681 at 2

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h2622.pdf>.

Note**:** This bill was enacted December 4, 2003.

National Consumer Credit Reporting System Improvement Act of 2003 (S. 1753)

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s1753.pdf>.

Note**:** This bill is superseded by H.R. 2622. (above)

Consumer Identity and Information Security Act of 2003 (H.R. 2617)

Purpose**:** To protect American consumers from identity theft and other forms of fraud.

Description**:** This bill would prohibit: displaying social security numbers; requiring the transmission of social security numbers over the Internet unless the connection is secured or the number encrypted; requiring users to authenticate on websites using their social security number, and displaying the social security number in communications with the individual. It would impose a duty to truncate account numbers on receipts and a duty on card issuers to use procedures to verify the identity of consumers when they request an additional card after a change of address. There would be a duty on consumer reporting agencies to disseminate fraud alerts.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h2617.pdf>.

Consumer Privacy Protection Act of 2003 (H.R. 1636)

Description**:** This bill is a re-introduction of the bill entitled *Consumer Privacy Protection Act* of 2002 (H.R. 4678).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h1636.pdf>.

Identify Theft Victims Assistance Act of 2003 (S. 1581)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Victims Assistance Act* of 2002 (H.R. 5424[107], S. 1742[107]).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s1581.pdf>.

Identify Theft Victims Assistance Act of 2003 (S. 1533[108])

Purpose**:** This bill is a re-introduction of the bill entitled *Identity Theft Victims Assistance Act* of 2002 (H.R. 5424[107], S. 1742[107]).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s1533.pdf>.

Prevent Identity Theft From Affecting Lives and Livelihoods (PITFALL) Act (H.R. 3296, S. 1749[108])

Purpose**:** To amend various provisions of the *Consumer Credit Protection Act* to provide relief for victims of identity theft, and for other purposes.

Description**:** This Act would remove liability for victims of identity theft following issuance of a no-fault letter by a credit agency upon completion of its investigation. It would impose a duty on credit reporting agencies to remove information on the transactions for which the victim is not liable. The bill would also impose a duty on debt collectors to stop collection actions once they have received a no-fault letter.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s1749.pdf>.

1.1.10. Bills introduced in 2004

Social Security Number Privacy and Identity Theft Prevention Act of 2004 (H.R. 2971, S. 2801)

Description**:** This bill is a re-introduction of the bill entitled *Social Security Number Privacy and Identity Theft Prevention Act* of 2001 (H.R. 2036, S. 1014).

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s2801.pdf>.

Social Security Number Privacy and Protection Act of 2004 (H.R. 4846)

Purpose**:** To reduce the risk of identity theft by limiting the use of Social Security account numbers on certain government-issued identification cards and government documents.

Description**:** The bill would mandate the alteration of the forms used by persons presenting themselves for registration under the *Military Selective Service Act.* It would also mandate that the Social Security account number be removed from Medicare, Medicaid (SSA title XIX), SCHIP and veterans health care identification cards. It expresses Congress' sense of concern regarding removal of social security account numbers from identification and claims cards used by health insurers.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/h4846.pdf>.

Anti-phishing Act of 2004 (S. 2636)

Purpose**:** To criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing.

Description**:** This bill would create an offence which is committed when an individual creates or procures the creation of a website or domain name which represents itself as a legitimate online business without the authority or approval of the registered owner of such business; and uses that website or domain name to solicit means of identification from any person. There would be a second offence which is committed when a person who knowingly and with the intent to engage in activity constituting fraud or identity theft under federal or state law: (1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet location tool referring or linking users to an online location on the World Wide Web that falsely purports to belong to or be associated with a legitimate online business; and (3) solicits means of identification from the recipient.

Text**:** <http://www.govtrack.us/data/us/bills.text/108/s2636.pdf>.

1.1.11. Bills introduced in 2005

Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers Beyond Borders Act of 2005 (S. 1608)

Purpose**:** To enhance Federal Trade Commission enforcement against illegal spam, spyware, and cross-border fraud and deception, and for other purposes.

Description**:** This bill proposes to include in the term "unfair or deceptive acts or practices" those acts or practices involving foreign commerce that: 1) cause or are likely to cause reasonably foreseeable injury within the United States; or 2) involve material conduct occurring within the United States. It would grant the FTC various powers to help its cooperation with foreign law enforcement agencies and the Attorney General.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s1608.pdf>.

Software Principles Yielding Better Levels of Consumer Knowledge Act (S. 687)

Purpose**:** To regulate the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes.

Description**:** This bill would make it unlawful to: install software on a protected computer without user consent; to mislead a user into installing software; to install software which is not removable through usual program removal functions and to install software which surreptitiously tracks the user or displays ads without giving the source. It contains liability limits for different parties, such as Internet Service Providers, OEMs and anti-spyware vendors. Any violation of this bill would be considered an unfair or deceptive act or practice.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s687.pdf>.

Securely Protect Yourself Against Cyber Trespass Act (H.R. 29)

Purpose**:** To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

Description**:** This bill would make it unlawful to engage in certain unfair or deceptive practices such as: 1) taking unsolicited control of a computer; 2) modifying computer settings; 3) collecting personally identifiable information; 4) inducing the owner or authorized user to disclose personally identifiable information; 5) inducing the unsolicited installation of computer software and 6) removing or disabling a security, anti-spyware, or anti-virus technology. It would also be unlawful to install or execute, without the user's consent, any information collection program which displays ads.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h29.pdf>.

Internet Spyware (I-SPY) Prevention Act of 2005 (H.R. 744)

Purpose**:** To amend title 18, United States Code, to discourage spyware, and for other purposes.

Description**:** This bill would prohibit intentionally accessing or exceeding authorized access to a protected computer by causing software to be installed and using that software to further a federal criminal offence, obtaining personal information with intent to defraud a person or cause damage to a protected computer or compromising the security of the computer. It would also prohibit any person from bringing a civil action under state law premised upon the defendant's violating this Act

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h744.pdf>.

Methamphetamine and Identity Theft Study Act of 2005 (H.R. 3325, S. 884)

Purpose**:** To conduct a study evaluating whether there are correlations between the commission of methamphetamine crimes and identity theft crimes.

Description**:** This bill **would** direct the Attorney General to create statistics evaluating whether there is a connection between methamphetamine and the commission of identity theft crimes. The study would have to look at sentencing if an individual commits both types of crimes, establishing a clearinghouse for the exchange of information on crimes involving both and whether methamphetamine users are more likely to use certain identity theft techniques.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3325.pdf>.

Identity Theft Relief Act of 2005 (H.R. 3804)

Purpose**:** To amend the *Internal Revenue Code* of 1986 to provide a 100 percent deduction for expenses related to identity theft.

Description**:** This bill would create a new tax deduction for all identity theft expenses arising from a fraud committed or attempted using identifying information without authority.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3804.pdf>.

Comprehensive Identity Theft Prevention Act (S. 768)

Purpose**:** To provide for comprehensive identity theft prevention.

Description**:** This bill would establishe The Office of Identity Theft, to have civil jurisdiction over any covered person who collects, maintains, sells, or transfers sensitive personal information, or attempts to collect, maintain, sell, or transfer sensitive personal information. It would require "data merchants" to register with the Office and that they put in place a dependable authentication process for each third party whom the data merchant permits to have access to consumer's sensitive personal information. The bill would also require the use of passwords to access consumers' sensitive personal information and notification of unauthorized accesses to unencrypted personal information. The solicitation, display, sale, purchase, or use of, and access to, Social Security Numbers would be prohibited.

Text**:** <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid= f:s768is.txt.pdf>.

Consumer Privacy Protection Act of 2005 (H.R. 1263)

Description**:** This bill is a re-introduction of the bill entitled *Consumer Privacy Protection Act* of 2003 (H.R. 1636).

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h1263.pdf>.

Notification of Risk to Personal Data Act (S. 1326)

Purpose**:** To require agencies, and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breaches pose a significant risk of identity theft.

Description**:** This bill would require any agency or person that owns or licenses sensitive personal information to implement reasonable security and notification procedures and practices to protect sensitive personal information from unauthorized access, destruction, use, modification, or disclosure and to notify any resident whose sensitive personal information was compromised. If an agency does not own or license the sensitive personal information it would have notify the entity from which the information was obtained. The bill would create civil remedies for failure to notify.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s1326.pdf>.

Identity Theft Protection Act (S. 1408)

Purpose**:** To strengthen data protection and safeguards, require data breach notification, and further prevent identity theft.

Description**:** This bill would require any entity that acquires, maintains, or utilizes sensitive personal information to implement a program for security that includes administrative, technical, and physical safeguards. It would also direct the FTC to create regulations that require procedures for authenticating the credentials of any third party who accesses the information. Entities would have to report breaches to the FTC and to consumer reporting agencies and post a report on their website, and to consumers depending on the characteristics of the breach. The bill would also impose a duty on consumer reporting agencies to add a security freeze on credit reports when requested by a consumer. It would prohibit entities from soliciting a social security number from an individual unless there is a specific use of that number for which no other identifier reasonably can be used. It also would prohibit the display of social security numbers by entities and by states on driver's licences.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s1408.pdf>.

Information Protection and Security Act (H.R. 1080, S. 500)

Purpose**:** To regulate information brokers and protect individual rights with respect to personally identifiable information.

Description**:** This bill would direct the FTC to promulgate regulations governing the conduct of information brokers. These regulations would include rules: (1) requiring procedures for maximum data accuracy, confidentiality, user authentication and tracking, the prevention and detection of illegal or unauthorized activity, and mitigation of potential harm to individuals and (2) giving users a right of access and correction to the information. Violations of these regulations would be treated as unfair and deceptive practices. The bill would permits states to bring civil actions against violators, and would create a private right of action for individuals injured as a result of the violation of these regulations.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s500.pdf>.

Regional ID Theft Task Force Act of 2005 (H.R. 4244)

Purpose**:** To provide for grants for regional task forces to more effectively investigate and prosecute identity theft and other economic crimes.

Description**:** The bill **would** direct the Attorney General to make grants to coalitions of federal, state, and local law enforcement agencies to establish regional task forces to more effectively investigate and prosecute identity theft and other economic crimes.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h4244.pdf>.

Anti-phishing Act of 2005 (H.R. 1099, S. 472)

Description**:** This bill is a re-introduction of the bill entitled *Anti-phishing Act* of 2004 (S. 2636).

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h1099.pdf>.

To amend title XVIII of the Social Security Act to permit Medicare beneficiaries upon request to use an identification number other than a social security account number under the Medicare... (H.R. 92)

Purpose**:** To amend title XVIII of the *Social Security Act* to permit Medicare beneficiaries upon request to use an identification number other than a social security account number under the Medicare Program in order to deter identity theft.

Description**:** This bill would direct the Secretary of Health and Human Services to use another identifier than the Social Security Number and to provide a Medicare card that contains that number.

Text**:** <http://www.govtrack.us/congress/bill.xpd?bill=h109-92>.

Data Accountability and Trust Act (DATA) (H.R. 4127)

Purpose**:** To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

Description**:** This bill would require the FTC to promulgate regulations that require each person engaged in interstate commerce to implement policies and procedures regarding information security practices for the treatment and protection of personal information. This bill would also create special requirements for data brokers.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h4127.pdf>.

Financial Privacy Protection Act of 2005 (S. 1594)

Purpose**:** To require financial services providers to maintain customer information security systems and to notify customers of unauthorized access to personal information, and for other purposes.

Description**:** This bill would require financial institutions to implement a security system to prevent any breach of their customer information. It would prescribe guidelines for the notification of consumers in case of an unauthorized access to customer information. There would be a right of a civil action for consumers affected, injunctions against financial institutions in violation and civil enforcement actions by state Attorneys General. A duty would be imposed on consumer reporting agencies to place a fraud alert on consumer files upon notification by a consumer. Users of consumer reports would be prohibited from taking any adverse action with respect to a consumer based solely on the inclusion of a fraud alert.

Text**:** <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1594is.txt.pdf>.

Consumer Notification and Financial Data Protection Act of 2005 (H.R. 3374)

Purpose**:** To provide for the uniform and timely notification of consumers whose sensitive financial personal information has been placed at risk by a breach of data security, to enhance data security safeguards, to provide appropriate consumer mitigation services and for other purposes.

Description**:** This bill would impose an obligation on financial institutions to implement security measures to protect the confidentiality of sensitive financial personal information against any unauthorized use that is reasonably likely to result in harm or substantial inconvenience to such consumer.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3374.pdf>.

Financial Data Protection Act of 2005 (H.R. 3997, S. 2169)

Purpose**:** To amend the *Fair Credit Reporting Act* to provide for secure financial data, and for other purposes.

Description**:** This bill would impose an obligation on "consumer reporters" to implement security measures to protect personal information maintained, serviced, or communicated by or on the reporter's behalf against any unauthorized use reasonably likely to result in substantial harm or inconvenience to the consumer. The definition of "consumer reporter" includes financial institutions, consumer reporting agencies and data brokers.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s2169.pdf>.

Note**:** Bill H.R. 3997 is entitled "*Financial Data Protection Act* of 2006".

Personal Data Privacy and Security Act of 2005 (S. 1789)

Purpose**:** To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access and misuse of personally identifiable information.

Description**:** This bill would make fraud and related activity in connection with unauthorized access to sensitive personally identifiable information a predicate offence. It would require data brokers to provide access and correction mechanisms to consumers. The bill subjects business entities that collect information on 10,000 or more U.S. persons to implement a Data Privacy and Security Program. Entities would have to notify consumers about security breaches. If they license the data breached, they must notify the licensee. Other notifications would be required depending on the characteristics of the breach.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s1789.pdf>.

Education for Retirement Security Act of 2005 (H.R. 392, S. 924)

Purpose**:** To establish a grant program to enhance the financial and retirement literacy of mid-life and older Americans and to reduce financial abuse and fraud among such Americans, and for other purposes.

Description**:** The bill would provide that the Secretary of Health and Human Services award grants to eligible entities to provide financial education programs to mid-life and older individuals, to enhance their financial knowledge and reduce financial abuse and fraud.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s924.pdf>.

Financial Data Security Act of 2005 (H.R. 3375)

Purpose**:** To amend the *Fair Credit Reporting Act* to provide for secure financial data, and for other purposes.

Description**:** This bill **would** impose a duty on consumer reporting agencies and data brokers to implement reasonable policies and procedures to protect the security and confidentiality of a consumer's sensitive financial information against unauthorized use. It would also impose a duty to notify consumers, other consumer reporting agencies, law enforcement agencies and third parties of security breaches.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3375.pdf>.

Identity Theft Prevention Act of 2005 (H.R. 220)

Description**:** This bill is a re-introduction of the bill entitled *Identity Theft Protection Act* of 2001 (H.R. 220).

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h220.pdf>.

Social Security Number Privacy and Identity Theft Prevention Act of 2005 (H.R. 1745)

Description**:** This bill is a re-introduction of the bill entitled *Social Security Number Privacy and Identity Theft Prevention Act* of 2004 (H.R. 2971, S. 2801).

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h1745.pdf>.

Consumer Data Security and Notification Act of 2005 (H.R. 3140)

Purpose**:** To expand the protections for sensitive personal information in federal law to cover the information collection and sharing practices of unregulated information brokers, to enhance information security requirements for consumer reporting agencies and information brokers, and to require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information, and for other purposes.

Description**:** This bill would impose an obligation on consumer reporting agencies to respect the privacy of consumers and protect the security and confidentiality of their non public personal information. It would impose an obligation on consumer reporting agencies to notify consumers of security breaches and unauthorized access to sensitive consumer information, unless the information is encrypted. Financial institutions would have a duty to notify consumers, law enforcement and the primary federal financial regulatory agency if they discover a security breach.

Text**:** <http://www.govtrack.us/congress/bill.xpd?bill=h109-3140>.

Consumer Access Rights Defense Act (CARD) of 2005 (H.R. 3501)

Purpose**:** To require financial institutions and financial service providers to notify customers of the unauthorized use of personal financial information, and for other purposes.

Description**:** This bill would impose a duty on agencies, or persons engaged in interstate commerce, that own, license, or collect data containing personal information, to notify individuals of security breaches or unauthorized access to their personal information. It would impose a duty on consumer reporting agencies to put an extended fraud alert on the credit report of an individual who submits evidence of a notification that personal financial information has or may have been compromised

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3501.pdf>.

Social Security Number Protection Act of 2005 (H.R. 1078)

Description**:** This bill is a re-introduction of the bill entitled *Social Security Number Protection Act* of 2002 (H.R. 4513)

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h1078.pdf>.

Financial Services Regulatory Relief Act of 2005 (H.R. 3505)

Purpose**:** To provide regulatory relief and improve productivity for insured depository institutions, and for other purposes.

Description**:** This bill would permit alleged offenders to dispute the validity of any alleged bad cheque violation where the alleged offender knows, or has reasonable cause to believe, that the alleged bad cheque violation is the result of theft or forgery of the cheque, identity theft, or other fraud that is not the result of their own conduct.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h3505.pdf>.

Privacy Act of 2005 (S. 116)

Purpose**:** To require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes.

Description**:** This bill would prohibit the sale and disclosure of personally identifiable information by a commercial entity to a non-affiliated third party except with the consent of the individual. The display, sale, or purchase of Social Security Numbers without the affirmatively expressed consent of the individual would be prohibited, as would the display of these numbers on cheques, driver's licences or motor vehicle registrations issued by governmental agencies. It would also prohibits a commercial entity from refusing to provide

goods or services if an individual does not provide a Social Security Number and sets criminal and civil damages for misuse of this number. Financial institutions would be prohibited from selling non-public personal financial information and the sale of health information by certain entities would also be prohibited.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s116.pdf>.

Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (S. 256)

Purpose**:** To amend title 11 of the United States Code, and for other purposes.

Description**:** The bankruptcy court would be able to protect, for cause, certain information, in order to protect against identity theft.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s256.pdf>.

1.1.12. Bills introduced in 2006

Credit Repair Organizations Act Technical Corrections Act (H.R. 5445)

Purpose**:** To provide clarification relating to credit monitoring services.

Description**:** This bill would impose a duty on "credit repair" organizations to disclose to consumers their rights in regards to their credit report. Consumers would have the right to cancel credit monitoring contracts without penalty.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h5445.pdf>.

Cyber-Security Enhancement and Consumer Data Protection Act of 2006 (H.R. 5318)

Purpose**:** To amend title 18, United States Code, to better assure cyber-security, and for other purposes.

Description**:** This bill would remove the requirement that a protected computer be used for interstate commerce for certain offences. A new offence, to conspire to commit a cyber-crime, would be created. The bill would also create an offence for whomever possesses data in electronic form and fails to notify law enforcement of a major security breach. It would increase sentences for certain cyber-crimes and allocates more funds to law enforcement agencies for training and investigating crimes committed with computers.

Text**:** <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h5318ih.txt.pdf>.

Notification of Risk to Personal Data Act (S. 751)

Description**:** This bill is a re-introduction of the bill entitled *Notification of Risk to Personal Data Act* (S. 1326)

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s751.pdf>.

Prevention of Fraudulent Access to Phone Records Act (H.R. 4943)

Purpose**:** To prohibit fraudulent access to telephone records.

Description: This bill would make it an offence to obtain or attempt to obtain customer proprietary network information relating to any other person by false pretences. It also would be an offence to sell customer proprietary network information obtained in such a manner. This bill would limit telecommunications carriers' uses of customer proprietary network information and require them to notify consumers of any breach of the provisions of this Act.

Text**:** <http://www.govtrack.us/data/us/bills.text/109/h4943.pdf>.

USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (H.R. 3199)

Purpose**:** To extend and modify authorities needed to combat terrorism, and for other purposes.

Description**:** A provision of this bill would expand the circumstances under which the interception of wire, oral, or electronic communications would be authorized to cover identity theft offences

Text**:** <http://www.govtrack.us/congress/bill.xpd?bill=h109-3199>.

Note**:** This bill was enacted March 9, 2006.

Social Security Number Misuse Prevention Act (S. 29)

Purpose**:** To amend title 18, United States Code, to limit the misuse of Social Security numbers, to establish criminal penalties for such misuse, and for other purposes.

Description**:** This bill would prohibit the display, sale, or purchase of Social Security Numbers without the express consent of the individual. The display of Social Security Numbers on cheques issued by governmental agencies and inmate access to these numbers would also be prohibited. Commercial entities would be prohibited from requiring individuals to provide a Social Security Number and from refusing to provide services or goods if individuals refuse to provide it. There would be criminal penalties for the misuse of Social Security Numbers and civil penalties against individuals who violate the Act.

Text**:** <http://www.govtrack.us/congress/bill.xpd?bill=s109-29>.

Financial Services Regulatory Relief Act of 2006 (S. 2856)

Description**:** This bill is a re-introduction of the bill entitled *Financial Services Regulatory Relief Act* of 2005 (H.R. 3505)

Text**:** <http://www.govtrack.us/data/us/bills.text/109/s2856.pdf>.

Telephone Records and Privacy Protection Act of 2006 (H.R. 4709)

Purpose: Create criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

Description: This bill would amend the federal criminal code to prohibit the obtaining, trafficking, in interstate or foreign commerce, of confidential phone records information.

Text: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills &docid=f:h4709enr.txt.pdf

1.2. State Legislation

1.2.1. California

1.2.1.1. The Penal Code of California19

False Personation and Cheats

Section 528 criminalizes personation in the context of marriage. Section 529 criminalizes personation when the offender becomes a bailiff or surety; uses a written instrument or commits an act which would make the person falsely personated liable.

Section 529a criminalizes the production and use of counterfeit certificates of birth and certificates of baptism knowing them to be counterfeit. It also criminalizes the use of genuine birth and baptism certificates to personate a living or deceased person.

Section 529.5 criminalizes manufacturing, selling, offering for sale, or transferring any document purporting to be a government-issued identification card with knowledge that the document is not a government-issued document.

Section 529.7 criminalizes helping another to obtain a driver's license, identification card, vehicle registration certificate, or any other official document issued by the Department of Motor Vehicles, with knowledge that the person obtaining the document is not entitled to the document.

Section 530 criminalizes personating another to obtain an advantage with intent to convert the same to his or her own use, or to that of another person, or to deprive the true owner thereof.

Section 530.5 criminalizes the wilful obtainment by any person of personal identifying information, of another person, and use of 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. The section also criminalizes acquisition, possession and trafficking of personal information with intent to defraud. It criminalizes trafficking of personal information when the trafficker has actual knowledge that it will be used to defraud. Mail theft, as defined in Section 1705 of Title 18 of the United States Code is also criminalized.

This section also requires that court records reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

[19] Penal Code of California, online:<http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=pen&codebody=&hits=20>.

The section also shields interactive computer services or access software providers from liability if their services are used to acquire, transfer, convey or retain personal information.

Section 530.55 defines a "person" as a natural person, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

It also defines “personal identifying information” as “any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification”.

Section 530.6 gives the right to an individual who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used to initiate a law enforcement investigation, by contacting the local law enforcement agency that has jurisdiction over his or her actual residence or place of business and which shall take a police report of the matter, and provide the complainant with a copy of that report. It also permits a victim to obtain a determination of his or her factual innocence by a court and to get it to remove the name and associated personal identifying information contained in court records, files, and indexes accessible by the public.

Section 530.8 gives identity theft victims the right to obtain information about any account opened in their name by an identity thief when the victim presents a police report. This information includes the personal information the thief used to open the account.

Section 531 criminalizes the fraudulent conveyance of any lands, tenements, or hereditaments, goods or chattels or any right or interest. Section 531a criminalizes executing, or getting another to execute, any instrument with intent to defraud.

Section 532 criminalizes defrauding, knowingly and by design, by any false or fraudulent representation or pretence, any other person of money, labour, or property, whether real or personal, or causing or procuring others to report falsely of his or her wealth or mercantile character.

Section 532a criminalizes knowingly making or causing to be made, either directly or indirectly or through any agency whatsoever, any false statement in writing, with intent that it shall be relied upon, respecting the financial condition of the person making the statement. It also criminalizes accepting such a statement knowing that it is a false statement.

Section 532b criminalizes falsely representing himself or herself as a veteran or ex-serviceman of any war in which the United States was engaged.

Sections 538d, 538e, 538f and 538g criminalize using uniforms, signs, badges, etc of certain groups such as firemen, law enforcement agencies and public utilities.

1.2.1.2. The Civil Code of the State of California20

Obligations Imposed By Law

Section 1725 prohibits requiring a person paying with a negotiable instrument to provide a credit card as a condition of acceptance of the negotiable instrument, or recording the number of the credit card. It also prohibits requiring a person from signing a statement to the effect that such a credit card be charged in case the negotiable instrument is returned as not valid.

Credit Cards

Section 1747.06 imposes a duty on credit card issuers to verify the address of a consumer: 1) if the address received is different from the address sent with a credit card solicitation and 2) if a request for a new credit card is received within 10 days of a change of address request.

Section 1747.08 prohibits requesting, or requiring as a condition to accepting the credit card as payment, the cardholder to write any personal identification information upon the credit card transaction form or otherwise.

Section 1747.09 imposes a duty on organizations which accept credit card payments to print no more than the five last digits of the credit or debit card, or the expiration date.

Section 1798.79.9 makes prohibits any entity or person from requesting personal information on victims from a Victim service provider. Victim service providers are nongovernmental organizations or entities that provides shelter, programs, or services at low cost, no cost, or on a sliding scale to victims of domestic violence, dating violence, sexual assault, or stalking, or to their children.

Obligations of Consumer Credit Reporting Agencies

Section 1785.10 requires consumer reporting agencies to provide consumers with access to their file.

Section 1785.11 limits the circumstances in which a consumer reporting agency can provide a credit report.

[20] Civil Code of the State of California: online <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20>.

Section 1785.11.1 gives consumers the right to place a security alert on their credit report by making a request in writing or by telephone to a consumer credit reporting agency. The "security alert" notifies a recipient of the credit report that the consumer's identity may have been used without the consumer's consent. It also imposes a duty on credit grantors to take reasonable steps to verify the consumer's identity before extending credit. In the security alert, the consumer may request to be contacted at a specified phone number by credit grantors before they may extend credit. This section imposes a duty on credit grantors to contact the individual at the specified number.

Section 1785.11.2 gives consumers the right to place a security freeze on their credit report by making a request in writing by certified mail to a consumer credit reporting agency. The consumer reporting agency must provide the consumer with a personal identification number or password which can be used to grant access to the credit report to specific parties. If a security freeze is in place, information from a consumer's credit report may not be released to a third party without prior express authorization from the consumer.

Section 1785.11.3 imposes a duty on consumer reporting agencies not to modify the name, date of birth, social security number, and address without sending a written confirmation of the change to the consumer when a security freeze has been placed on the credit report.

Section 1785.11.4 imposes a duty on credit report resellers and amalgamators to respect security freezes placed on credit reports.

Section 1785.11.8 gives consumers the right to opt out of having their name included in lists prepared for credit card solicitations.

Section 1785.14 imposes a duty on consumer reporting agencies to implement procedures to ensure compliance with their duties. These procedures require that prospective users of the information identify themselves, certify the purposes for which the information is sought and certify that the information will be used for no other purposes.

Section 1785.15.3 imposes a duty on consumer reporting agencies to notify consumers of their rights when they are contacted by a consumer who has reason to believe he or she may be a victim of identity theft. It also gives the consumer the right to request a credit report monthly for twelve months upon the presentation of a police report prepared pursuant to Section 530.6 of the *Penal Code* or a valid investigative report made by a Department of Motor Vehicles investigator with peace officer status.

Section 1785.16 imposes a duty on consumer reporting agencies to investigate any information in a credit report disputed by a consumer and to remove such if the information if it is found to be inaccurate.

Section 1785.16.1 imposes a duty on consumer reporting agencies to delete from a credit report inquiries initiated as the result of identity theft.

Section 1785.16.2 prohibits the sale or transfer by creditors of consumer debts to a debt collector, if the consumer is a victim of identity theft and creditor has received notice.

Section 1785.19 provides consumers with recourses against individuals who wilfully obtain access to a file or to their data, other than as provided in Section 1785.11.

Section 1788.18 provides that a "debtor" means a natural person, firm, association, organization, partnership, business trust, company, corporation, or limited liability company from which a debt collector seeks to collect a debt. This provides non-persons the same rights as an individual to contest any debt that resulted from identity theft.

Requirements on Users of Consumer Credit Reports

Section 1785.20.3 imposes a duty on credit report users to take reasonable steps to verify the accuracy of the consumer's first and last name, address, or social security number provided on the application when such information does not match information in the credit report.

Debt Collector Responsibilities

Sections 1788.10, 1788.11, 1788.12, 1788.13, 1788.14 and 1788.15 limit the conduct and practices of debt collectors.

Section 1788.18 imposes a duty on debt collectors to cease collection until they have conducted a review when they are provided with different written statements that the individual was the victim of identity theft. Upon receiving such a statement, the debt collector must review and consider all of the information provided by the debtor and other information available to the debt collector in its file or from the creditor.

Accounting of Disclosures

Section 1798.29 imposes a duty on agencies which own or license computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Customer Records

Section 1798.81 imposes a duty to on businesses to take all reasonable steps to destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information which is no longer to be retained by the business by: 1) shredding, 2) erasing, or 3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Section 1798.82 imposes on businesses the same security breach notification obligations as s. 1798.29 imposes on public agencies.

Section 1798.83 requires businesses which disclose a consumer's personal information to a third party, to disclose to consumers, upon receiving a request to that effect, the recipients of that information and a description of the categories of the information disclosed.

Confidentiality of Social Security Numbers

Section 1798.85 prohibits publicly displaying social security numbers, printing them on any card required for the individual to access products or services, requiring their transmission over unencrypted connection requiring them to access a Internet Web site unless another identifier is required or printing them on any mailing, unless state or federal law requires the Social Security Number to be on the document to be mailed. It also gives the right to individuals to request that their Social Security Number stop being used as described above. The section also makes any waiver of rights under this section void and unenforceable.

Confidentiality of Driver's License Information

Section 1798.90.1 imposes limits to the use and retention of data encoded on driver's licenses or identification cards issued by the Department of Motor Vehicles.

Identity Theft

Section 1798.93 gives identity theft victims the right to file a cross-complaint to establish that the person is a victim of identity theft in connection with a claimant's claim. The victim may obtain an injunction restraining the claimant from collecting or attempting to collect from the victim on that claim, from enforcing or attempting to enforce any security interest or other interest in the victim's property in connection with that claim, or from enforcing or executing on any judgment against the victim on that claim.

1.2.1.3. Financial Code21

Loan Regulations

Section 22342 requires that loan solicitations shall be mailed in envelopes with no indication that a negotiable instrument is contained in the mailing. Envelopes shall be marked with "do not forward" instructions to the postal service in the event that the intended addressee is no longer at the location.

California Financial Information Privacy Act

Section 4052.5 prohibits financial institutions from selling, sharing, transferring or otherwise disclosing non-public personal information to or with any non-affiliated third

[21] Financial Code, online:<http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=fin&codebody=&hits=20>.

parties without the explicit prior consent of the consumer to whom the non-public personal information relates.

1.2.1.4. Family Code22

Section 2024.5 gives the right to the petitioner or respondent to redact any social security number from any pleading, attachment, document, or other written material filed with the court pursuant to a petition for dissolution of marriage, nullity of marriage, or legal separation.

1.2.1.5. Health and Safety Code 23

Section 103526 requires that individuals who request a certified copy of a birth or death record provide a notarized statement sworn under penalty of perjury that the requester is an authorized person.

1.2.1.6. Business and Professions Code[24]

Section 350 creates the Department of Consumer Affairs, an Office of Privacy Protection under the direction of the Director of Consumer Affairs and the Secretary of the State and the Consumer Services Agency. This department must: 1) receive complaints from individuals concerning any person obtaining, compiling, maintaining, using, disclosing, or disposing of personal information in a manner that may be potentially unlawful, and 2) provide information to consumers on effective ways of handling complaints that involve violations of privacy-related laws, including identity theft and identity fraud.

1.2.1.7. Elections Code[25]

Section 2188.5 prohibits sending voter information outside of the United States or making it available in any way electronically to persons outside the United States, including, but not limited to, access over the Internet.

1.2.1.8. Bills

Elder and dependent adults: theft or embezzlement by caretaker (AB 484)

Purpose: An act to amend Section 368 of the Penal Code, and to amend Section 15656 of the Welfare and Institutions Code, relating to elder and dependent adult abuse.

---

[22] Family Code, online: <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=fam&codebody=&hits=20>.

[23] Health and Safety Code, online: <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=hsc&codebody=&hits=20>.

[24] Business and Professions Code, online <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=bpc&codebody=&hits=20>.

[25] *Elections Code*, online: <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=elec&codebody=&hits=20>.

Description: This bill would introduce a new offence for caretakers who violate any provision of law proscribing theft, embezzlement, forgery, or fraud, or who violate Section 530.5 proscribing identity theft, with respect to the property or personal identifying information of an elder or a dependent adult, and who know or reasonably should know that the victim is an elder or a dependent adult.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_0451-0500/ab_484_bill_20050504_amendedasm.pdf

Cogdill Crime (AB 618)

Purpose: An act to amend Section 7480 of the Government Code, relating to crime.

Description: This bill would provide that a law enforcement agency may also request, and a bank, credit union, or savings association must then provide, surveillance photos, photographs and video recordings of a person accessing the crime victim's financial account via an ATM or from within the financial institution, as specified.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_0601-0650/ab_618_bill_20060605_amended_sen.pdf

Identity theft: California State University employees (AB 786)

Purpose: An act to repeal and amend Section 1798.29 of the Civil Code, relating to identity theft.

Description: This bill would require the California State University system to provide an employee, upon request, with four hours of time off with pay following a disclosure by the university that there is, or could have been, a breach of security of employee personal information data, as specified.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_0751-0800/ab_786_bill_20050218_introduced.pdf

Elder abuse (AB 916)

Purpose: An act to add Section 368.5 to the Penal Code, relating to crime.

Description: This bill would increase the penalties for certain violations of section 368.5 of the *Penal Code*.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_0901-0950/ab_916_bill_20050705_amended_sen.pdf

Identity theft (AB 946)

Purpose: An act to amend Section 530.5 of the Penal Code, relating to crime.

Description: This bill would increase the fines for offences in which an individual wilfully obtains personal identifying information about another person and uses that information for any unlawful purpose. The fines that may be imposed for the commission of this crime would be increased to $2,000, and $20,000.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_0901-0950/ab_946_bill_20050218_introduced.pdf

Identity theft (AB 1581)

Purpose: An act to amend Section 530.5 of the Penal Code, relating to identity theft.

Description: This bill would make it a felony or a misdemeanour to acquire, transfer, or retain the personal information of 100 or more persons with the intent to defraud.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_1551-1600/ab_1581_bill_20050504_amended_asm.pdf

Consumer credit reporting (AB 1694)

Purpose: An act to add sections 1785.11.5 and 1785.15.5 to the Civil Code, relating to consumer credit reporting.

Description: This bill would require consumer reporting agencies to provide free "Security Freezes" at the request of a consumer whose personal information was breached by a computerized data system. The bill would authorize the consumer credit reporting agency to charge the agency responsible for the breach, and would require the consumer to submit a copy of notification of the breach to the consumer credit reporting agency, as a condition of receiving the security freeze

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_1651-1700/ab_1694_bill_20050421_amended_asm.pdf

Instruction: economics (AB 1950)

Purpose: An act to add Section 51220.7 to the Education Code, relating to pupil instruction.

Description: This bill would allow school districts to include instruction related to the understanding of personal finances, including, but not limited to budgeting, savings, credit, and identity theft.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_1901-1950/ab_1950_bill_20060526_amended_asm.pdf

Debt collection: businesses: identity theft (AB 2043)

Purpose: An act to amend Sections 1788.2 and 1788.18 of the Civil Code, relating to debt collection.

Description: Debt collectors would have to stop collecting a consumer debt when an alleged debtor provides information relating to the alleged debtor's status as a victim of identity theft under this bill. it would extend this protection to a natural person, firm, association, organization, partnership, business trust, company, corporation, or limited liability company.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2001-2050/ab_2043_bill_20060607_amended_sen.pdf

Identity theft (AB 2333)

Purpose: An act to amend Section 530.5 of the Penal Code, relating to identity theft.

Description: This bill would create a new offence for a person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information of ten or more other persons.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2301-2350/ab_2333_bill_20060330_amended_asm.pdf

Privacy protection: personal identification documents (AB 2561)

Purpose: An act to add Article 13 (commencing with Section 11147) to Chapter 1 of Part 1 of Title 1 of the Government Code, relating to privacy.

Description: This bill would require the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable identification credentials.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2551-2600/ab_2561_bill_20060502_amended_asm.pdf

Crime (AB 2886)

Purpose: An act to amend Section 530.5 of, and to add Section 593h to the Penal Code, relating to crime.

Description: This bill would provide that a second or subsequent violation of the provision that makes it an offence to wilfully obtain personal identifying information about another person and use that information for any unlawful purpose, is punishable by a fine not to exceed $10,000, imprisonment in the state prison for sixteen months, or two or three years, or by both that fine and imprisonment.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2851-2900/ab_2886_bill_20060526_amended_asm.pdf

Identity theft (AB 2919)

Purpose: An act to amend Section 529 of, and to add Sections 530.55 and 13012.6 to, the Penal Code, relating to identity theft.

Description: This bill would change the definition of the offence "where any person who falsely personates another and does any act whereby, if done by the person falsely personated, might make him or her liable to any suit or prosecution is punishable by a fine" to include acts that might make the person falsely personated liable to arrest or a criminal charge. It would require the Department of Justice to include statistics on arrests for identity theft crimes in its annual report to the Governor. It would change the possible penalties for "unlawful phishing".

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2901-2950/ab_2919_bill_20060515_amended_asm.pdf

Identity Theft (AB 2956)

Purpose: An act to amend Sections 502.6 and 530.5 of the Penal Code, relating to identity.

Description: This bill would increase the penalties for "skimming". It would also expand the offence "any person who with the intent to defraud acquires, transfers, or retains possession of the personal identifying information of another person" to include conveying, sale and trafficking of the information and it increases the possible penalties.

Text: http://www.leginfo.ca.gov/pub/bill/asm/ab_2951-3000/ab_2956_bill_20060503_amended_asm.pdf

Child identity theft (SB 346)

Purpose: An act to amend Section 530.5 of the Penal Code, relating to crime and Section 300 of the Welfare and Institutions Code, relating to dependent children .

Description: This bill would provide that a child whose parent or legal guardian has used the personal identifying information of the child in violation of identity theft criminal provisions may be adjudged a dependent child of the juvenile court.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_0301-0350/sb_346_bill_20050418_amended_sen.pdf

***Identity Information Protection Act* of 2005** (SB 682, SB 768)

Purpose: An act to add Article 4 (commencing with Section 1798.9) to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to privacy.

Description: This bill would require RFID enabled identification documents, or identification documents which enable personal information to be read remotely, to meet specified requirements. It would create a new offence for a person or entity that *intentionally* remotely reads or attempts to remotely read a person's identification document using radio waves without his or her knowledge.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050815_amended_asm.pdf

Identity Theft (SB 839)

Purpose: An act to amend Sections 186.22, 529, 530.5, 530.6, and 786 of, and to add Sections 540, 541, 530.55, and 1203.051 to, the Penal Code, relating to crime.

Description: This bill would add forgery of a counterfeit access card and misdemeanour fraudulent use of an access card to the list of offences qualifying for a pattern of criminal gang activity and would expand the list of offences uses to define a "criminal street gang" and a "pattern of criminal gang activity" to include several offences relating to theft of access cards and personal information. It would change the definition of the offence “where any person who falsely personates another and does any act whereby, if done by the person falsely personated, might make him or her liable to any suit or prosecution is punishable by a fine” to include acts that might make the person falsely personated liable to arrest or a criminal charge. It would also change the definition of another person in the offence “a person who wilfully obtains personal identifying information about another person, and uses that information for any unlawful purpose” to include natural persons living and deceased, and organizations, associations, business relationships and other legal entities. Every person convicted of a felony violation of, or conspiracy to violate these provisions, would be punishable by an additional two-year term of imprisonment in the state prison for each prior felony conviction of, or conviction of conspiracy to violate specified provisions.

This bill would also change the penalties for phishing. Persons convicted of a high-technology related offence primarily through the use of a computer have to pay a $250 forensic computer analysis fee. This bill would provide that proper jurisdiction for any crime properly joinable with a violation of identity theft provisions, theft of, or fraudulent use of access cards or account information, forgery of access cards, or trafficking in card making equipment would also include the county in which the victim resided at the time the offence was committed. Probation would not be granted nor would the execution or imposition of a sentence be suspended for a person who has been convicted of a felony

violation of provisions relating to personal identifying information if he or she has a prior felony conviction for a violation of those provisions.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_0801-0850/sb_839_bill_20060105_amended_sen.pdf

Identity Theft (SB 852)

Purpose: An Act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to identity theft.

Description: This bill would require an agency, or a person or business conducting business in California that owns, licenses, or collects computerized data that includes the personal information of a California resident, to notify the resident of any breach of the security of the data, as specified, regardless of whether the data was computerized when it was acquired.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_0851-0900/sb_852_bill_20050622_amended_asm.pdf

Dissolution of marriage: financial declarations (SB 1015)

Purpose: An Act to amend Section 2024.6 of, and to add Section 2024.7 of, the Family Code, and to amend Section 68085.1 of the Government Code, relating to dissolution of marriage, and declaring the urgency thereof, to take effect immediately.

Description: This bill would require the court, upon request of a party, to redact the social security number, residence address, and certain financial information of a party, as specified.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1001-1050/sb_1015_bill_20060425_amended_asm.pdf

Crime statistics (SB 1390)

Purpose: An act to add Section 13012.6 to the Penal Code, relating to crime statistics.

Description: This bill would require the Department of Justice to include statistics on arrests for identity theft crimes in its annual report to the Governor.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1351-1400/sb_1390_bill_20060405_amended_sen.pdf

Identity theft: financial crimes (SB 1495)

Purpose: An act to amend Section 530.5 of the Penal Code, relating to identity theft.

Description: This bill would create a new offence when a person wilfully obtains the personal identifying information of another person who is less than 18 years of age if the victim's age was known, or should have been known to that person, and uses that information for unlawful purposes without the consent of the victim.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1451-1500/sb_1495_bill_20060327_amended_sen.pdf

Telephone records: obtaining telephone calling pattern record or list (SB 1651)

Purpose: An act to amend Sections 1798.92 and 1798.93 of the Civil Code, and to add Section 530.1 to the Penal Code, relating to telephone records.

Description: This bill would make the wilful obtaining of another person's telephone calling pattern record or list, as defined, without the consent of that person, a public offence, punishable by fine or imprisonment or both, thereby imposing a state-mandated local program by creating a new crime. It would authorize a person to bring an action against any individual, business association, partnership, limited partnership, corporation, limited liability company, or other legal entity that wilfully obtains a telephone calling pattern record or list of that person, and upon proof by a preponderance of evidence, recover actual damages, attorney's fees, costs, and any other equitable relief that the court deems appropriate.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1651-1700/sb_1651_bill_20060224_introduced.pdf

Pupil's instruction: Internet safety curriculum guidelines (SB 1740)

Purpose: An act to add Chapter 5.8 (commencing with Section 51950) to Part

Description: The bill would provide that the State Department of Education develop and maintain Internet safety curriculum guidelines on the role of computer spyware in identity theft and financial fraud.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1701-1750/sb_1740_bill_20060503_amended_sen.pdf

Information privacy: consumer credit reports (SB 1744)

Purpose: An act to amend Section 1785.11.2 of the Civil Code, relating to information privacy.

Description: This bill would require consumer credit reporting agencies establish an electronic contact method and a toll-free telephone number for taking requests from consumers to temporarily lift security freezes and would require that requests that are made

pursuant to these methods during business hours be effective within fifteen minutes, except as specified.

Text: http://www.leginfo.ca.gov/pub/bill/sen/sb_1701-1750/sb_1744_bill_20060504_amended_sen.pdf

2. STATUTE EXCERPTS

2.1. Federal

2.1.1. *Identity Theft and Assumption Deterrence Act*, 18 U.S.C § 1028

§ 003. Identity Theft.

(a) Establishment of Offense.--Section 1028(a) of title 18, United States Code, is amended--

(1) in paragraph (5), by striking "or" at the end;
(2) in paragraph (6), by adding "or" at the end;
(3) in the flush matter following paragraph (6), by striking "or attempts to do so,"; and
(4) by inserting after paragraph (6) the following:

"(7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law;".

(d) Definitions.--Subsection (d) of section 1028 of title 18, United States Code, is amended to read as follows:

"(d) In this section--

"(1) the term `document-making implement' means any implement, impression, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;
"(2) the term `identification document' means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

"(3) the term `means of identification' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any--

"(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
"(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
"(C) unique electronic identification number, address, or routing code; or
"(D) telecommunication identifying information or access device (as defined in section 1029(e));

"(4) the term `personal identification card' means an identification document issued by a State or local government solely for the purpose of identification;
"(5) the term `produce' includes alter, authenticate, or assemble; and
"(6) the term `State' includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States.".

§ 005. Centralized Complaint and Consumer Education Service for Victims of Identity Theft. [NOTE: 18 USC 1028 note.]

(a) In <<NOTE: Deadline.>> General.--Not later than 1 year after the date of enactment of this Act, the Federal Trade Commission shall establish procedures to--

(1) log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification (as defined in section 1028 of title 18, United States Code, as amended by this Act) have been assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act;
(2) provide informational materials to individuals described in paragraph (1); and
(3) refer complaints described in paragraph (1) to appropriate entities, which may include referral to--

(A) the 3 major national consumer reporting agencies; and
(B) appropriate law enforcement agencies for potential law enforcement action.

(b) Authorization of Appropriations.--There are authorized to be appropriated such sums as may be necessary to carry out this section.

2.1.2. *Identity Theft Penalty Enhancement Act*, 18 U.S.C § 1001

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding after section 1028, the following:

''§ 1028A. Aggravated identity theft

''(a) OFFENSES.—

''(1) IN GENERAL.—Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

''(2) TERRORISM OFFENSE.—Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

''(b) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;

''(3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of title 28.

''(c) DEFINITION.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of—

''(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans);

''(2) section 911 (relating to false personation of citizenship);

''(3) section 922(a)(6) (relating to false statements in connection with the acquisition of a firearm);

''(4) any provision contained in this chapter (relating to fraud and false

statements), other than this section or section 1028(a)(7);
‘‘(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud);
‘‘(6) any provision contained in chapter 69 (relating to nationality and citizenship);
‘‘(7) any provision contained in chapter 75 (relating to passports and visas);
‘‘(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823) (relating to obtaining customer information by false pretenses);
‘‘(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card);
‘‘(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or
‘‘(11) section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307(b), 1320a–7b(a), and 1383a) (relating to false statements relating to programs under the Act).’’.

(b) AMENDMENT TO CHAPTER ANALYSIS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1028 the following new item: ‘‘1028A. Aggravated identity theft.’’.

(c) APPLICATION OF DEFINITIONS FROM SECTION 1028.—Section 1028(d) of title 18, United States Code, is amended by inserting ‘‘and section 1028A’’ after ‘‘In this section’’.

SEC. 5. DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.

(a) IN GENERAL.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and amend its guidelines and its policy statements to ensure that the guideline offense levels and enhancements appropriately punish identity theft offenses involving an abuse of position.

(b) REQUIREMENTS.—In carrying out this section, the United States Sentencing Commission shall do the following:

(1) Amend U.S.S.G. section 3B1.3 (Abuse of Position of Trust of Use of Special Skill) to apply to and punish offenses in which the defendant exceeds or abuses the authority of his or her position in order to obtain unlawfully or use without authority any means of identification, as defined section 1028(d)(4) of title 18, United States Code.
(2) Ensure reasonable consistency with other relevant directives, other sentencing guidelines, and statutory provisions.
(3) Make any necessary and conforming changes to the sentencing guidelines.
(4) Ensure that the guidelines adequately meet the purposes of sentencing set forth in section 3553(a)(2) of title 18, United States Code.

2.1.3. *Fair and Accurate Credit Transactions Act* (FACTA), U.S.C. § 1681

§ 605. Requirements relating to information contained in consumer reports [15 U.S.C. §1681c]

(f) *Indication of dispute by consumer*. If a consumer reporting agency is notified pursuant to section 623(a)(3) [§ 1681s-2] that information regarding a consumer who was furnished to the agency is disputed by the consumer, the agency shall indicate that fact in each consumer report that includes the disputed information.

(g) Truncation of Credit Card and Debit Card Numbers

(1) I*n general*. Except as otherwise provided in this subsection, no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.

(2) *Limitation*. This subsection shall apply only to receipts that are electronically printed, and shall not apply to transactions in which the sole means of recording a credit card or debit card account number is by handwriting or by an imprint or copy of the card.

(3) *Effective date*. This subsection shall become effective--

(A) 3 years after the date of enactment of this subsection, with respect to any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions that is in use before January 1, 2005; and

(B) 1 year after the date of enactment of this subsection, with respect to any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions that is first put into use on or after January 1, 2005.

(h) Notice of Discrepancy in Address

(1) *In general*. If a person has requested a consumer report relating to a consumer from a consumer reporting agency described in section 603(p), the request includes an address for the consumer that substantially differs from the addresses in the file of the consumer, and the agency provides a consumer report in response to the request, the consumer reporting agency shall notify the requester of the existence of the discrepancy.

(2) Regulations

(A) *Regulations required.* The Federal banking agencies, the National Credit Union Administration, and the Commission shall jointly, with respect to the entities that are subject to their respective enforcement authority under section 621, prescribe regulations providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice of discrepancy under paragraph (1).

(B) *Policies and procedures to be included.* The regulations prescribed under subparagraph (A) shall describe reasonable policies and procedures for use by a user of a consumer report--

(i) to form a reasonable belief that the user knows the identity of the person to whom the consumer report pertains; and

(ii) if the user establishes a continuing relationship with the consumer, and the user regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of discrepancy pertaining to the consumer was obtained, to reconcile the address of the consumer with the consumer reporting agency by furnishing such address to such consumer reporting agency as part of information regularly furnished by the user for the period in which the relationship is established.

§ 605A. Identity theft prevention; fraud alerts and active duty alerts [15 U.S.C. §1681c-1]

(a) One-call Fraud Alerts

(1) *Initial alerts.* Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency described in section 603(p) that maintains a file on the consumer and has received appropriate proof of the identity of the requester shall--

(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, for a period of not less than 90 days, beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose; and

(B) refer the information regarding the fraud alert under this paragraph to each of the other consumer reporting agencies described in section 603(p), in accordance with procedures developed under section 621(f).

(2) *Access to free reports.* In any case in which a consumer reporting agency includes a fraud alert in the file of a consumer pursuant to this subsection, the consumer reporting agency shall--

(A) disclose to the consumer that the consumer may request a free copy of the file of the consumer pursuant to section 612(d); and

(B) provide to the consumer all disclosures required to be made under section 609, without charge to the consumer, not later than 3 business days after any request described in subparagraph (A).

(b) Extended Alerts

(1) *In general.* Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who submits an identity theft report to a consumer reporting agency described in section 603(p) that maintains a file on the consumer, if the agency has received appropriate proof of the identity of the requester, the agency shall--

(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, during the 7-year period beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period and the agency has received appropriate proof of the identity

of the requester for such purpose;

(B) during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer or such representative requests that such exclusion be rescinded before the end of such period; and

(C) refer the information regarding the extended fraud alert under this paragraph to each of the other consumer reporting agencies described in section 603(p), in accordance with procedures developed under section 621(f).

(2) *Access to free reports.* In any case in which a consumer reporting agency includes a fraud alert in the file of a consumer pursuant to this subsection, the consumer reporting agency shall--

(A) disclose to the consumer that the consumer may request 2 free copies of the file of the consumer pursuant to section 612(d) during the 12-month period beginning on the date on which the fraud alert was included in the file; and

(B) provide to the consumer all disclosures required to be made under section 609, without charge to the consumer, not later than 3 business days after any request described in subparagraph (A).

(c) *Active duty alerts.* Upon the direct request of an active duty military consumer, or an individual acting on behalf of or as a personal representative of an active duty military consumer, a consumer reporting agency described in section 603(p) that maintains a file on the active duty military consumer and has received appropriate proof of the identity of the requester shall--

(1) include an active duty alert in the file of that active duty military consumer, and also provide that alert along with any credit score generated in using that file, during a period of not less than 12 months, or such longer period as the Commission shall determine, by regulation, beginning on the date of the request, unless the active duty military consumer or such representative requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose;

(2) during the 2-year period beginning on the date of such request, exclude the active duty military consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer requests that such exclusion be rescinded before the end of such period; and

(3) refer the information regarding the active duty alert to each of the other consumer reporting agencies described in section 603(p), in accordance with procedures developed under section 621(f).

(d) *Procedures.* Each consumer reporting agency described in section 603(p) shall establish policies and procedures to comply with this section, including procedures that inform consumers of the availability of initial, extended, and active duty alerts and procedures that

allow consumers and active duty military consumers to request initial, extended, or active duty alerts (as applicable) in a simple and easy manner, including by telephone.

(e) *Referrals of alerts.* Each consumer reporting agency described in section 603(p) that receives a referral of a fraud alert or active duty alert from another consumer reporting agency pursuant to this section shall, as though the agency received the request from the consumer directly, follow the procedures required under—

(1) paragraphs (1)(A) and (2) of subsection (a), in the case of a referral under subsection (a)(1)(B);

(2) paragraphs (1)(A), (1)(B), and (2) of subsection (b), in the case of a referral under subsection (b)(1)(C); and

(3) paragraphs (1) and (2) of subsection (c), in the case of a referral under subsection (c)(3).

(f) *Duty of reseller to reconvey alert.* A reseller shall include in its report any fraud alert or active duty alert placed in the file of a consumer pursuant to this section by another consumer reporting agency.

(g) *Duty of other consumer reporting agencies to provide contact information.* If a consumer contacts any consumer reporting agency that is not described in section 603(p) to communicate a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, the agency shall provide information to the consumer on how to contact the Commission and the consumer reporting agencies described in section 603(p) to obtain more detailed information and request alerts under this section.

(h) Limitations on Use of Information for Credit Extensions

(1) Requirements for initial and active duty alerts-

(A) *Notification.* Each initial fraud alert and active duty alert under this section shall include information that notifies all prospective users of a consumer report on the consumer to which the alert relates that the consumer does not authorize the establishment of any new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph (B).

(B) Limitation on Users

(i) *In general*. No prospective user of a consumer report that includes an initial fraud alert or an active duty alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or grant any increase in credit limit on an existing credit account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

(ii) *Verification.* If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before

authorizing any new credit plan or extension described in clause (i) in the name of such consumer, a user of such consumer report shall contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft.

(2) Requirements for Extended Alerts

(A) *Notification.* Each extended alert under this section shall include information that provides all prospective users of a consumer report relating to a consumer with–

(i) notification that the consumer does not authorize the establishment of any new credit plan or extension of credit described in clause (i), other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph (B); and
(ii) a telephone number or other reasonable contact method designated by the consumer.

(B) *Limitation on users.* No prospective user of a consumer report or of a credit score generated using the information in the file of a consumer that includes an extended fraud alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, unless the user contacts the consumer in person or using the contact method described in subparagraph (A)(ii) to confirm that the application for a new credit plan or increase in credit limit, or request for an additional card is not the result of identity theft.

§ 605B. Block of information resulting from identity theft [15 U.S.C. §1681c-2]

(a) *Block.* Except as otherwise provided in this section, a consumer reporting agency shall block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft, not later than 4 business days after the date of receipt by such agency of--

(1) appropriate proof of the identity of the consumer;
(2) a copy of an identity theft report;
(3) the identification of such information by the consumer; and
(4) a statement by the consumer that the information is not information relating to any transaction by the consumer.

(b) *Notification.* A consumer reporting agency shall promptly notify the furnisher of information identified by the consumer under subsection (a)--

(1) that the information may be a result of identity theft;
(2) that an identity theft report has been filed;
(3) that a block has been requested under this section; and
(4) of the effective dates of the block.

(c) Authority to Decline or Rescind

(1) *In general.* A consumer reporting agency may decline to block, or may rescind any block, of information relating to a consumer under this section, if the consumer reporting agency reasonably determines that--

(A) the information was blocked in error or a block was requested by the consumer in error;

(B) the information was blocked, or a block was requested by the consumer, on the basis of a material misrepresentation of fact by the consumer relevant to the request to block; or

(C) the consumer obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

(2) *Notification to consumer*. If a block of information is declined or rescinded under this subsection, the affected consumer shall be notified promptly, in the same manner as consumers are notified of the reinsertion of information under section 611(a)(5)(B).

(3) *Significance of block.* For purposes of this subsection, if a consumer reporting agency rescinds a block, the presence of information in the file of a consumer prior to the blocking of such information is not evidence of whether the consumer knew or should have known that the consumer obtained possession of any goods, services, or money as a result of the block.

(d) Exception for Resellers

(1) *No reseller file.* This section shall not apply to a consumer reporting agency, if the consumer reporting agency--

(A) is a reseller;

(B) is not, at the time of the request of the consumer under subsection (a), otherwise furnishing or reselling a consumer report concerning the information identified by the consumer; and

(C) informs the consumer, by any means, that the consumer may report the identity theft to the Commission to obtain consumer information regarding identity theft.

(2) *Reseller with file.* The sole obligation of the consumer reporting agency under this section, with regard to any request of a consumer under this section, shall be to block the consumer report maintained by the consumer reporting agency from any subsequent use, if--

(A) the consumer, in accordance with the provisions of subsection (a), identifies, to a consumer reporting agency, information in the file of the consumer that resulted from identity theft; and

(B) the consumer reporting agency is a reseller of the identified information.

(3) *Notice*. In carrying out its obligation under paragraph (2), the reseller shall promptly provide a notice to the consumer of the decision to block the file. Such notice shall contain the name, address, and telephone number of each consumer reporting agency from which the consumer information was obtained for resale.

(e) *Exception for verification companies*. The provisions of this section do not apply to a check services company, acting as such, which issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payments, except that, beginning 4 business days after receipt of information

described in paragraphs (1) through (3) of subsection (a), a check services company shall not report to a national consumer reporting agency described in section 603(p), any information identified in the subject identity theft report as resulting from identity theft.
(f) *Access to blocked information by law enforcement agencies.* No provision of this section shall be construed as requiring a consumer reporting agency to prevent a Federal, State, or local law enforcement agency from accessing blocked information in a consumer file to which the agency could otherwise obtain access under this title.

§ 607. Compliance procedures [15 U.S.C. § 1681e]
(a) *Identity and purposes of credit users*. Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of section 605 [§ 1681c] and to limit the furnishing of consumer reports to the purposes listed under section 604 [§ 1681b] of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 604 [§ 1681b] of this title.

§ 609. Disclosures to consumers [15 U.S.C. § 1681g]
(e) Information Available to Victims

(1) *In general.* For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph (3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph (2), a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to--

(A) the victim;
(B) any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or
(C) any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) *Verification of identity and claim*. Before a business entity provides any information under paragraph (1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph (1), the victim shall provide to the business entity--

(A) as proof of positive identification of the victim, at the election of the business entity–

(i) the presentation of a government-issued identification card;
(ii) personally identifying information of the same type as was provided to the business entity by the unauthorized person; or
(iii) personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

(B) as proof of a claim of identity theft, at the election of the business entity--
(i) a copy of a police report evidencing the claim of the victim of identity theft; and
(ii) a properly completed--
(I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or
(II) an affidavit of fact that is acceptable to the business entity for that purpose.

§ 610. Conditions and form of disclosure to consumers [15 U.S.C. § 1681h]

(a) In General

(1) *Proper identification.* A consumer reporting agency shall require, as a condition of making the disclosures required under section 609 [§ 1681g], that the consumer furnish proper identification.

(2) *Disclosure in writing.* Except as provided in subsection (b), the disclosures required to be made under section 609 [§ 1681g] shall be provided under that section in writing.

§ 612. Charges for certain disclosures [15 U.S.C. § 1681j] ***See also 16 CFR Part 610 69 Fed. Reg. 35467 (06/24/04)***

(a) Free Annual Disclosure

(1) Nationwide Consumer Reporting Agencies

(A) *In general.* All consumer reporting agencies described in subsections (p) and (w) of section 603 shall make all disclosures pursuant to section 609 once during any 12-month period upon request of the consumer and without charge to the consumer.

§ 628. Disposal of records [15 U.S.C. §1681w]

(a) Regulations

(1) *In general.* Not later than 1 year after the date of enactment of this section, the Federal banking agencies, the National Credit Union Administration, and the Commission with respect to the entities that are subject to their respective enforcement authority under section 621, and the Securities and Exchange Commission, and in coordination as described in paragraph (2), shall issue final regulations requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation.

2.1.4. *Fraud and related activity in connection with identification documents*, 18 U.S.C. § 1028

(a) Whoever, in a circumstance described in subsection (c) of this section—

(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;

(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false authentication features for use in false identification documents, document-making implements, or means of identification;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is—

(1) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is—

(A) the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—

(i) an identification document or authentication feature issued by or under the authority of the United States; or

(ii) a birth certificate, or a driver's license or personal identification card;

(B) the production or transfer of more than five identification documents, authentication features, or false identification documents;

(C) an offense under paragraph (5) of such subsection; or
(D) an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period;

(2) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 5 years, or both, if the offense is—
(A) any other production, transfer, or use of a means of identification, an identification document,,[1] authentication feature, or a false identification document; or
(B) an offense under paragraph (3) or (7) of such subsection;

(3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—
(A) to facilitate a drug trafficking crime (as defined in section 929 (a)(2)); **(B)** in connection with a crime of violence (as defined in section 924 (c)(3)); or
(C) after a prior conviction under this section becomes final;

(4) a fine under this title or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under section 2331 (5) of this title) or an act of international terrorism (as defined in section 2331 (1) of this title);

(5) in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and

(6) a fine under this title or imprisonment for not more than one year, or both, in any other case.

(c) The circumstance referred to in subsection (a) of this section is that—
(1) the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document;
(2) the offense is an offense under subsection (a)(4) of this section; or
(3) either—
(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or
(B) the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.

(d) In this section and section 1028A—
(1) the term “authentication feature” means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority

on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;

(2) the term "document-making implement" means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;

(3) the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

(4) the term "false identification document" means a document of a type intended or commonly accepted for the purposes of identification of individuals that—

(A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and

(B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;

(5) the term "false authentication feature" means an authentication feature that—

(A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit;

(B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or

(C) appears to be genuine, but is not;

(6) the term "issuing authority"—

(A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and

(B) includes the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization;

(7) the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number,

government passport number, employer or taxpayer identification number;
(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(C) unique electronic identification number, address, or routing code; or
(D) telecommunication identifying information or access device (as defined in section 1029 (e));

(8) the term "personal identification card" means an identification document issued by a State or local government solely for the purpose of identification;
(9) the term "produce" includes alter, authenticate, or assemble;
(10) the term "transfer" includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others;
(11) the term "State" includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States; and
(12) the term "traffic" means—

(A) to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or
(B) to make or obtain control of with intent to so transport, transfer, or otherwise dispose of.

(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

(f) Attempt and Conspiracy.— Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

(g) Forfeiture Procedures.— The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(h) Forfeiture; Disposition.— In the circumstance in which any person is convicted of a violation of subsection (a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification.

(i) Rule of Construction.— For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.

2.1.5. *Internet False Identification Act of 2000*, 18 U.S.C § 1021

SEC. 3. FALSE IDENTIFICATION.
Section 1028 of title 18, United States Code, is amended—
(1) in subsection (c)(3)(A), by inserting ‘‘, including the transfer of a document by electronic means’’ after ‘‘commerce’’; and
(2) in subsection (d)—
(A) in paragraph (1), by inserting ‘‘template, computer file, computer disc,’’ after ‘‘impression,’’;
(B) in paragraph (5), by striking ‘‘and’’ after the semicolon;
(C) by redesignating paragraph (6) as paragraph (8);
(D) by redesignating paragraphs (3) through (5) as paragraphs (4) through (6), respectively;
(E) by inserting after paragraph (2) the following:
‘‘(3) the term ‘false identification document’ means a document of a type intended or commonly accepted for the purposes of identification of individuals that—
‘‘(A) is not issued by or under the authority of a governmental entity; and
‘‘(B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;’’; and
(F) by inserting after paragraph (6), as redesignated, the following:
‘‘(7) the term ‘transfer’ includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others; and’’.

2.1.6. *Privacy Act of 1971*, 5 U.S.C. § 552a

§ 552a. Records maintained on individuals
(b) Conditions of disclosure
No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--
(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
(2) required under section 552 of this title;
(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;
(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting

record, and the record is to be transferred in a form that is not individually identifiable;
(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
(11) pursuant to the order of a court of competent jurisdiction; or
(12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.

(e) Agency requirements
Each agency that maintains a system of records shall—

…
(10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

2.1.7. *Prohibition on release and use of certain personal information from State motor vehicle records*, 18 U.S.C. § 2721

(a) In General.— A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:

(1) personal information, as defined in 18 U.S.C. 2725 (3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
(2) highly restricted personal information, as defined in 18 U.S.C. 2725 (4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That

subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States.

(b) Permissible Uses.— Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321–331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows:

(1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

(2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

(3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—

(A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

(B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

(4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

(5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

(6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

(7) For use in providing notice to the owners of towed or impounded vehicles.

(8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

(9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.

(10) For use in connection with the operation of private toll transportation facilities.
(11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
(12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
(13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
(14) For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.

(c) Resale or Redisclosure.— An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

(d) Waiver Procedures.— A State motor vehicle department may establish and carry out procedures under which the department or its agents, upon receiving a request for personal information that does not fall within one of the exceptions in subsection (b), may mail a copy of the request to the individual about whom the information was requested, informing such individual of the request, together with a statement to the effect that the information will not be released unless the individual waives such individual's right to privacy under this section.

(e) Prohibition on Conditions.— No State may condition or burden in any way the issuance of an individual's motor vehicle record as defined in 18 U.S.C. 2725 (1) to obtain express consent. Nothing in this paragraph shall be construed to prohibit a State from charging an administrative fee for issuance of a motor vehicle record.

2.1.8. *Health Insurance Portability and Accountability Act of 1996* (HIPAA), 42 U.S.C § 201

'SEC. 1171. For purposes of this part:

…

''(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—
The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that—

''(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

''(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or

future payment for the provision of health care to an individual, and—

''(i) identifies the individual; or

''(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

SEC. 242. HEALTH CARE FRAUD.

(a) OFFENSE.—

(1) IN GENERAL.—Chapter 63 of title 18, United States Code, is amended by adding at the end the following:

''§ 1347. Health care fraud

''Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice—

''(1) to defraud any health care benefit program; or

''(2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program,

in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 10 years, or both. If the violation results in serious bodily injury (as defined in section 1365 of this title), such person shall be fined under this title or imprisoned not more than 20 years, or both; and if the violation results in death, such person shall be fined under this title, or imprisoned for any term of years or for life, or both.''.

SEC. 244. FALSE STATEMENTS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1035. False statements relating to health care matters

''(a) Whoever, in any matter involving a health care benefit program, knowingly and willfully—

''(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or

''(2) makes any materially false, fictitious, or fraudulent statements or representations, or makes or uses any materially false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry,

in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 5 years, or both.

''SEC. 1173. (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.—

''(1) IN GENERAL.—The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for—

''(A) the financial and administrative transactions described in paragraph (2); and

''(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

''(2) TRANSACTIONS.—The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

''(A) Health claims or equivalent encounter information.

‘‘(B) Health claims attachments.
‘‘(C) Enrollment and disenrollment in a health plan.
‘‘(D) Eligibility for a health plan.
‘‘(E) Health care payment and remittance advice.
‘‘(F) Health plan premium payments.
‘‘(G) First report of injury.
‘‘(H) Health claim status.
‘‘(I) Referral certification and authorization.

‘‘(3) ACCOMMODATION OF SPECIFIC PROVIDERS.—The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

‘‘(b) UNIQUE HEALTH IDENTIFIERS.—

‘‘(1) IN GENERAL.—The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

‘‘(2) USE OF IDENTIFIERS.—The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

‘‘(c) CODE SETS.—

‘‘(1) IN GENERAL.—The Secretary shall adopt standards that—

‘‘(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

‘‘(B) establish code sets for such data elements if no code sets for the data elements have been developed.

‘‘(2) DISTRIBUTION.—The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

‘‘(d) SECURITY STANDARDS FOR HEALTH INFORMATION.—

‘‘(1) SECURITY STANDARDS.—The Secretary shall adopt security standards that—

‘‘(A) take into account—

‘‘(i) the technical capabilities of record systems used to maintain health information;

‘‘(ii) the costs of security measures;

‘‘(iii) the need for training persons who have access to health information;

‘‘(iv) the value of audit trails in computerized record systems; and

‘‘(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

''(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

''(2) SAFEGUARDS.—Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

''(A) to ensure the integrity and confidentiality of the information;

''(B) to protect against any reasonably anticipated—

''(i) threats or hazards to the security or integrity of the information; and

''(ii) unauthorized uses or disclosures of the information; and

''(C) otherwise to ensure compliance with this part by the officers and employees of such person.

''SEC. 1177. (a) OFFENSE.—A person who knowingly and in violation of this part—

''(1) uses or causes to be used a unique health identifier;

''(2) obtains individually identifiable health information relating to an individual; or

''(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

''(b) PENALTIES.—A person described in subsection (a) shall—

''(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

''(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

''(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) IN GENERAL.—Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.—The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

2.1.9. *Gramm-Leach-Bliley Act*, 12 U.S.C § 1811

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) PRIVACY OBLIGATION POLICY.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

SEC. 502. OBLIGATIONS WITH RESPECT TO DISCLOSURES OF PERSONAL INFORMATION.

(a) NOTICE REQUIREMENTS.—Except as otherwise provided in this subtitle, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 503.

(b) OPT OUT.—

(1) IN GENERAL.—A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2) EXCEPTION.—This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

(c) LIMITS ON REUSE OF INFORMATION.—Except as otherwise provided in this subtitle, a nonaffiliated third party that receives from a financial institution nonpublic

personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person
that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.
(d) LIMITATIONS ON THE SHARING OF ACCOUNT NUMBER INFORMATION FOR MARKETING PURPOSES.—A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction
account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.
(e) GENERAL EXCEPTIONS.—Subsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information—

(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with—

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, United States Code, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act, or (B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all

or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

SEC. 503. DISCLOSURE OF INSTITUTION PRIVACY POLICY.

(a) DISCLOSURE REQUIRED.—At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, of such financial institution's policies and practices with respect to—

(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed;

(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers. Such disclosures shall be made in accordance with the regulations prescribed under section 504.

(b) INFORMATION TO BE INCLUDED.—The disclosure required by subsection (a) shall include—

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 502 of this subtitle, and including—

(A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 502(e); and

(B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 501; and

(4) the disclosures required, if any, under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act.

SEC. 521. PRIVACY PROTECTION FOR CUSTOMER INFORMATION OF FINANCIAL INSTITUTIONS.

(a) PROHIBITION ON OBTAINING CUSTOMER INFORMATION BY FALSE PRETENSES.—It shall be a violation of this subtitle for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person—

(1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution;

(2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or

(3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

(b) PROHIBITION ON SOLICITATION OF A PERSON TO OBTAIN CUSTOMER INFORMATION FROM FINANCIAL INSTITUTION UNDER FALSE PRETENSES.—It shall be a violation of this subtitle to request a person to obtain customer information of a financial institution, knowing that the person will obtain, or attempt to obtain, the information from the institution in any manner described in subsection (a).

(c) NONAPPLICABILITY TO LAW ENFORCEMENT AGENCIES.—No provision of this section shall be construed so as to prevent any action by a law enforcement agency, or any officer, employee, or agent of such agency, to obtain customer information of a financial institution in connection with the performance of the official duties of the agency.

(d) NONAPPLICABILITY TO FINANCIAL INSTITUTIONS IN CERTAIN CASES.—No provision of this section shall be construed so as to prevent any financial institution, or any officer, employee, or agent of a financial institution, from obtaining customer information of such financial institution in the course of—

(1) testing the security procedures or systems of such institution for maintaining the confidentiality of customer information;

(2) investigating allegations of misconduct or negligence on the part of any officer, employee, or agent of the financial institution; or

(3) recovering customer information of the financial institution which was obtained or received by another person in any manner described in subsection (a) or (b).

(e) NONAPPLICABILITY TO INSURANCE INSTITUTIONS FOR INVESTIGATION OF INSURANCE FRAUD.—No provision of this section shall be construed so as to prevent any insurance institution, or any officer, employee, or agency of an insurance institution, from obtaining information as part of an insurance investigation into criminal activity, fraud, material misrepresentation, or material nondisclosure that is authorized for such institution under State law, regulation, interpretation, or order.

(f) NONAPPLICABILITY TO CERTAIN TYPES OF CUSTOMER INFORMATION OF FINANCIAL INSTITUTIONS.—No provision of this section shall be construed so as to prevent any person from obtaining customer information of a financial institution that otherwise is available as a public record filed pursuant to the securities laws (as defined in section 3(a)(47) of the Securities Exchange Act of 1934).

(g) NONAPPLICABILITY TO COLLECTION OF CHILD SUPPORT JUDGMENTS.—No provision of this section shall be construed to prevent any State-licensed private investigator, or any officer, employee, or agent of such private investigator, from obtaining customer information of a financial institution, to the extent reasonably necessary to collect child support from a person adjudged to have been delinquent in his or her obligations by a Federal or State court, and to the extent that such action by a State-licensed private investigator is not unlawful under any other Federal or State law or regulation, and has been authorized by an order or judgment of a court of competent jurisdiction.

2.1.10. *Social Security Number Confidentiality Act of 2000*, 31 U.S.C § 3301

SEC. 2. OPEN DISCLOSURE OF SOCIAL SECURITY ACCOUNT NUMBERS ON THE FACE OF GOVERNMENT CHECK MAILINGS PROHIBITED.
Section 3327 of title 31 of the United States Code (relating to general authority to issue checks and other drafts) is amended—

(1) by inserting ‘‘(a)’’ before ‘‘The Secretary’’; and
(2) by adding at the end the following new subsection:
‘‘(b) The Secretary of the Treasury shall take such actions as are necessary to ensure that Social Security account numbers (including derivatives of such numbers) are not visible on or through unopened mailings of checks or other drafts described in subsection (a) of this section.’’.

2.1.11. *Veterans Benefits, Health Care, and Information Technology Act of 2006*, 38 U.S.C § 101

SEC. 902. DEPARTMENT OF VETERANS AFFAIRS INFORMATION SECURITY PROGRAMS AND REQUIREMENTS.

(a) INFORMATION SECURITY PROGRAMS AND REQUIREMENTS.— Chapter 57 is amended by adding at the end the following new subchapter:

‘‘SUBCHAPTER III—INFORMATION SECURITY

‘‘§ 5724. Provision of credit protection and other services

‘‘(a) INDEPENDENT RISK ANALYSIS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

‘‘(2) If the Secretary determines, based on the findings of a risk analysis conducted under paragraph (1), that a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach, the Secretary shall provide credit protection services in accordance with the regulations prescribed by the Secretary under this section.

‘‘(b) REGULATIONS.—Not later than 180 days after the date of the enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, the Secretary shall prescribe interim regulations for the provision of the following in accordance with subsection (a)(2):

‘‘(1) Notification.

‘‘(2) Data mining.

‘‘(3) Fraud alerts.

‘‘(4) Data breach analysis.

‘‘(5) Credit monitoring.

‘‘(6) Identity theft insurance.

‘‘(7) Credit protection services.

‘‘(c) REPORT.—(1) For each data breach with respect to sensitive personal information processed or maintained by the Secretary, the Secretary shall promptly submit to the Committees on Veterans’ Affairs of the Senate and House of Representatives a report containing the findings of any independent risk analysis conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any services provided pursuant to subsection (b).

‘‘(2) In the event of a data breach with respect to sensitive personal information processed or maintained by the Secretary that is the sensitive personal information of a member of the Army, Navy, Air Force, or Marine Corps or a civilian officer or employee of the Department of Defense, the Secretary shall submit the report required under paragraph (1) to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives in addition to the Committees on Veterans’ Affairs of the Senate and House of Representatives.

‘‘§ 5725. Contracts for data processing or maintenance

‘‘(a) CONTRACT REQUIREMENTS.—If the Secretary enters into a contract for the performance of any Department function that requires access to sensitive personal information, the Secretary shall require as a condition of the contract that— ‘‘

(1) the contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract;

‘‘(2) the contractor, or any subcontractor for a subcontract of the contract, shall promptly notify the Secretary of any data breach that occurs with respect to such information.

‘‘(b) LIQUIDATED DAMAGES.—Each contract subject to the requirements of subsection (a) shall provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

‘‘(c) PROVISION OF CREDIT PROTECTION SERVICES.—Any amount collected by the Secretary under subsection (b) shall be deposited in or credited to the Department account from which the contractor was paid and shall remain available for obligation without fiscal year limitation exclusively for the purpose of providing credit protection services pursuant to section 5724(b) of this title.

2.1.12. *Fair Credit Reporting Act*, 15 U.S.C. § 1681

619. Obtaining information under false pretenses [15 U.S.C. § 1681q]
Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under title 18, United States Code, imprisoned for not more than 2 years, or both.

§ 620. Unauthorized disclosures by officers or employees [15 U.S.C. § 1681r]
Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined under title 18, United States Code, imprisoned for not more than 2 years, or both.

2.1.13. *Electronic Funds Transfer Act*, 15 U.S.C. § 1693

§ 1693g. Consumer liability
(a) Unauthorized electronic fund transfers; limit
A consumer shall be liable for any unauthorized electronic fund transfer involving the account of such consumer only if the card or other means of access utilized for such transfer was an accepted card or other means [sic] of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorized to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation. In no event, however, shall a consumer's liability for an unauthorized transfer exceed the lesser of—

(1) $50; or

(2) the amount of money or value of property or services obtained in such unauthorized electronic fund transfer prior to the time the financial institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable belief that an unauthorized electronic fund transfer involving the consumer's account has been or may be effected. Notice under this paragraph is sufficient when such steps have been taken as may be reasonably required in the ordinary course of business to provide the financial institution with the pertinent information, whether or not any particular officer, employee, or agent of the financial institution does in fact receive such information.

Notwithstanding the foregoing, reimbursement need not be made to the consumer for losses the financial institution establishes would not have occurred but for the failure of the consumer to report within sixty days of transmittal of the statement (or in extenuating circumstances such as extended travel or hospitalization, within a reasonable time under the circumstances) any unauthorized electronic fund transfer or account error which appears on the periodic statement provided to the consumer under section 1693d of this title. In addition, reimbursement need not be made to the consumer for losses which the financial institution establishes would not have occurred but for the failure of the consumer to report any loss or theft of a card or other means of access within two business days after the consumer learns of the loss or theft (or in extenuating circumstances such as extended travel or hospitalization, within a longer period which is

reasonable under the circumstances), but the consumer's liability under this subsection in any such case may not exceed a total of $500, or the amount of unauthorized electronic fund transfers which occur following the close of two business days (or such longer period) after the consumer learns of the loss or theft but prior to notice to the financial institution under this subsection, whichever is less.

(b) Burden of proof

In any action which involves a consumer's liability for an unauthorized electronic fund transfer, the burden of proof is upon the financial institution to show that the electronic fund transfer was authorized or, if the electronic fund transfer was unauthorized, then the burden of proof is upon the financial institution to establish that the conditions of liability set forth in subsection (a) of this section have been met, and, if the transfer was initiated after the effective date of section 1693c of this title, that the disclosures required to be made to the consumer under section 1693c (a)(1) and (2) of this title were in fact made in accordance with such section.

(c) Determination of limitation on liability

In the event of a transaction which involves both an unauthorized electronic fund transfer and an extension of credit as defined in section 1602 (e) of this title pursuant to an agreement between the consumer and the financial institution to extend such credit to the consumer in the event the consumer's account is overdrawn, the limitation on the consumer's liability for such transaction shall be determined solely in accordance with this section.

(d) Restriction on liability

Nothing in this section imposes liability upon a consumer for an unauthorized electronic fund transfer in excess of his liability for such a transfer under other applicable law or under any agreement with the consumer's financial institution.

(e) Scope of liability

Except as provided in this section, a consumer incurs no liability from an unauthorized electronic fund transfer.

§ 1693i. Issuance of cards or other means of access

(a) Prohibition; proper issuance

No person may issue to a consumer any card, code, or other means of access to such consumer's account for the purpose of initiating an electronic fund transfer other than—

(1) in response to a request or application therefor; or

(2) as a renewal of, or in substitution for, an accepted card, code, or other means of access, whether issued by the initial issuer or a successor.

(b) Exceptions

Notwithstanding the provisions of subsection (a) of this section, a person may distribute to a consumer on an unsolicited basis a card, code, or other means of access for use in initiating an electronic fund transfer from such consumer's account, if—

(1) such card, code, or other means of access is not validated;

(2) such distribution is accompanied by a complete disclosure, in accordance with section 1693c of this title, of the consumer's rights and liabilities which will apply if such card, code, or other means of access is validated;

(3) such distribution is accompanied by a clear explanation, in accordance with regulations of the Board, that such card, code, or other means of access is not

validated and how the consumer may dispose of such code, card, or other means of access if validation is not desired; and

(4) such card, code, or other means of access is validated only in response to a request or application from the consumer, upon verification of the consumer's identity.

(c) Validation

For the purpose of subsection (b) of this section, a card, code, or other means of access is validated when it may be used to initiate an electronic fund transfer.

§ 1693m. Civil liability

(a) Individual or class action for damages; amount of award

Except as otherwise provided by this section and section 1693h of this title, any person who fails to comply with any provision of this subchapter with respect to any consumer, except for an error resolved in accordance with section 1693f of this title, is liable to such consumer in an amount equal to the sum of—

(1) any actual damage sustained by such consumer as a result of such failure;

(2)

(A) in the case of an individual action, an amount not less than $100 nor greater than $1,000; or

(B) in the case of a class action, such amount as the court may allow, except that

(i) as to each member of the class no minimum recovery shall be applicable, and

(ii) the total recovery under this subparagraph in any class action or series of class actions arising out of the same failure to comply by the same person shall not be more than the lesser of $500,000 or 1 per centum of the net worth of the defendant; and

(3) in the case of any successful action to enforce the foregoing liability, the costs of the action, together with a reasonable attorney's fee as determined by the court.

(b) Factors determining amount of award

In determining the amount of liability in any action under subsection (a) of this section, the court shall consider, among other relevant factors—

(1) in any individual action under subsection (a)(2)(A) of this section, the frequency and persistence of noncompliance, the nature of such noncompliance, and the extent to which the noncompliance was intentional; or

(2) in any class action under subsection (a)(2)(B) of this section, the frequency and persistence of noncompliance, the nature of such noncompliance, the resources of the defendant, the number of persons adversely affected, and the extent to which the noncompliance was intentional.

(c) Unintentional violations; bona fide error

Except as provided in section 1693h of this title, a person may not be held liable in any action brought under this section for a violation of this subchapter if the person shows by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error.

(d) Good faith compliance with rule, regulation, or interpretation of Board or approval of duly authorized official or employee of Federal Reserve System
No provision of this section or section 1693n of this title imposing any liability shall apply to—

> **(1)** any act done or omitted in good faith in conformity with any rule, regulation, or interpretation thereof by the Board or in conformity with any interpretation or approval by an official or employee of the Federal Reserve System duly authorized by the Board to issue such interpretations or approvals under such procedures as the Board may prescribe therefor; or
> **(2)** any failure to make disclosure in proper form if a financial institution utilized an appropriate model clause issued by the Board,

notwithstanding that after such act, omission, or failure has occurred, such rule, regulation, approval, or model clause is amended, rescinded, or determined by judicial or other authority to be invalid for any reason.
(e) Notification to consumer prior to action; adjustment of consumer's account
A person has no liability under this section for any failure to comply with any requirement under this subchapter if, prior to the institution of an action under this section, the person notifies the consumer concerned of the failure, complies with the requirements of this subchapter, and makes an appropriate adjustment to the consumer's account and pays actual damages or, where applicable, damages in accordance with section 1693h of this title.
(f) Action in bad faith or for harassment; attorney's fees
On a finding by the court that an unsuccessful action under this section was brought in bad faith or for purposes of harassment, the court shall award to the defendant attorney's fees reasonable in relation to the work expended and costs.
(g) Jurisdiction of courts; time for maintenance of action
Without regard to the amount in controversy, any action under this section may be brought in any United States district court, or in any other court of competent jurisdiction, within one year from the date of the occurrence of the violation.

2.1.14. *Fair Credit Billing Act*, 15 U.S.C § 1601

§ 161. Correction of billing errors
.(a) If a creditor, within sixty days after having transmitted to an obligor a statement of the obligor's account in connection with an extension of consumer credit, receives at the address disclosed under section 127(b) (11) a written notice (other than notice on a payment stub or other payment medium supplied by the creditor if the creditor so stipulates with the
disclosure required under section 127(a) (8)) from the obligor in which the obligor.

> "(1) sets forth or otherwise enables the creditor to identify the name and account number (if any) of the obligor,
> "(2) indicates the obligor's belief that the statement contains a billing error and the amount of such billing error, and
> "(3) sets forth the reasons for the obligor's belief (to the extent applicable) that the statement contains a billing error,

the creditor shall, unless the obligor has, after giving such written notice and before the expiration of the time limits herein specified, agreed that the statement was correct.

> "(A) not later than thirty days after the receipt of the notice, send a written acknowledgment thereof to the obligor, unless the action required in subparagraph (B) is taken within such thirty-day period, and
> "(B) not later than two complete billing cycles of the creditor (in no event later than ninety days) after the receipt of the notice and prior to taking any action to collect the amount, or any part thereof, indicated by the obligor under paragraph (2) either –
>
> > "(i) make appropriate corrections in the account of the obligor, including the crediting of any finance charges on amounts erroneously billed, and transmit to the obligor a notification of such corrections and the creditor's explanation of any cage in the amount indicated by the obligor under paragraph (2) and, if any such change is made and the obligor so requests, copies of documentary evidence of the obligor's indebtedness; or
> > "(ii) send a written explanation or clarification to the obligor, after having conducted an investigation, setting forth to the extent applicable the reasons why the creditor believes the account of the obligor was correctly shown in the statement and, upon request of the obligor, provide copies of documentary evidence of the obligor's indebtedness. In the case of a billing error where the obligor alleges that the creditor's billing statement reflects goods not delivered to the obligor or his designee in accordance with the agreement made at the time of the transaction, a creditor may not construe such amount to be correctly shown unless he determines that such goods were actually delivered, mailed, or otherwise sent to the obligor and provides the obligor with a statement of such determination.
>
> After complying with the provisions of this subsection with respect to an alleged billing error, a creditor has no further responsibility under this section if the obligor continues to make substantially the same allegation with respect to such error.

2.1.15. *Fair Debt Collections Practices Act*, 15 U.S.C § 1601

§ 804. Acquisition of location information [15 USC 1692b]

Any debt collector communicating with any person other than the consumer for the purpose of acquiring location information about the consumer shall --
[…]

> (6) after the debt collector knows the consumer is represented by an attorney with regard to the subject debt and has knowledge of, or can readily ascertain, such attorney's name and address, not communicate with any person other than that attorney, unless the attorney fails to respond within a reasonable period of time to the communication from the debt collector.

§ 805. Communication in connection with debt collection [15 USC 1692c]

(a) COMMUNICATION WITH THE CONSUMER GENERALLY. Without the prior consent of the consumer given directly to the debt collector or the express permission of a court of competent jurisdiction, a debt collector may not communicate with a consumer in connection with the collection of any debt –

> (1) at any unusual time or place or a time or place known or which should be known to be inconvenient to the consumer. In the absence of knowledge of circumstances to the contrary, a debt collector shall assume that the convenient time for communicating with a consumer is after 8 o'clock antimeridian and before 9 o'clock postmeridian, local time at the consumer's location;
>
> (2) if the debt collector knows the consumer is represented by an attorney with respect to such debt and has knowledge of, or can readily ascertain, such attorney's name and address, unless the attorney fails to respond within a reasonable period of time to a communication from the debt collector or unless the attorney consents to direct communication with the consumer; or
>
> (3) at the consumer's place of employment if the debt collector knows or has reason to know that the consumer's employer prohibits the consumer from receiving such communication.

b) COMMUNICATION WITH THIRD PARTIES. Except as provided in section 804, without the prior consent of the consumer given directly to the debt collector, or the express permission of a court of competent jurisdiction, or as reasonably necessary to effectuate a postjudgment judicial remedy, a debt collector may not communicate, in connection with the collection of any debt, with any person other than a consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector.

(c) CEASING COMMUNICATION. If a consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector shall not communicate further with the consumer with respect to such debt, except --

> (1) to advise the consumer that the debt collector's further efforts are being terminated;
>
> (2) to notify the consumer that the debt collector or creditor may invoke specified remedies which are ordinarily invoked by such debt collector or creditor; or
>
> (3) where applicable, to notify the consumer that the debt collector or creditor intends to invoke a specified remedy.

If such notice from the consumer is made by mail, notification shall be complete upon receipt.

(d) For the purpose of this section, the term "consumer" includes the consumer's spouse, parent (if the consumer is a minor), guardian, executor, or administrator.

§ 806. Harassment or abuse [15 USC 1692d]

A debt collector may not engage in any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:

(1) The use or threat of use of violence or other criminal means to harm the physical person, reputation, or property of any person.

(2) The use of obscene or profane language or language the natural consequence of which is to abuse the hearer or reader.

(3) The publication of a list of consumers who allegedly refuse to pay debts, except to a consumer reporting agency or to persons meeting the requirements of section 603(f) or 604(3)[1] of this Act.

(4) The advertisement for sale of any debt to coerce payment of the debt.

(5) Causing a telephone to ring or engaging any person in telephone conversation repeatedly or continuously with intent to annoy, abuse, or harass any person at the called number.

(6) Except as provided in section 804, the placement of telephone calls without meaningful disclosure of the caller's identity.

2.1.15.1. Federal Trade Commission Act, *15 U.S.C. §§ 41-5826*

§ 45. Unfair methods of competition unlawful; prevention by Commission

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a (f)(3) of this title, Federal credit unions described in section 57a (f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227 (b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving

[26] *Federal Trade Commission Act*, 15 U.S.C. §§ 41-58, online: http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000041----000-.html.

commerce with foreign nations (other than import commerce) unless—

(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect—

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.

If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

2.2. California

2.2.1. *Penal Code*

528. Every person who falsely personates another, and in such assumed character marries or pretends to marry, or to sustain the marriage relation towards another, with or without the connivance of such other, is guilty of a felony.

529a. Every person who manufactures, produces, sells, offers, or transfers to another any document purporting to be either a certificate of birth or certificate of baptism, knowing such document to be false or counterfeit and with the intent to deceive, is guilty of a crime, and upon conviction therefor, shall be punished by imprisonment in the county jail not to exceed one year, or by imprisonment in the state prison. Every person who offers, displays, or has in his or her possession any false or counterfeit certificate of birth or certificate of baptism, or any genuine certificate of birth which describes a person then living or deceased, with intent to represent himself or herself as another or to conceal his or her true identity, is guilty of a crime, and upon conviction therefor, shall be punished by imprisonment in the county jail not to exceed one year.

529.5. (a) Every person who manufactures, sells, offers for sale, or transfers any document, not amounting to counterfeit, purporting to be a government-issued identification card or driver's license, which by virtue of the wording or appearance thereon could reasonably deceive an ordinary person into believing that it is issued by a government agency, and who knows that the document is not a government-issued document, is guilty of a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, or by a fine not exceeding one thousand dollars ($1,000), or by both the fine and imprisonment.

(b) Any person who, having been convicted of a violation of subdivision (a), is subsequently convicted of a violation of subdivision (a), is punishable for the subsequent conviction by imprisonment in a county jail not exceeding one year, or by a fine not exceeding five thousand dollars ($5,000), or by both the fine and imprisonment.

(c) Any person who possesses a document described in subdivision (a) and who knows that the document is not a government-issued document is guilty of a misdemeanor punishable by a fine of not less than one thousand dollars ($1,000) and not more than

two thousand five hundred dollars ($2,500). The misdemeanor fine shall be imposed except in unusual cases where the interests of justice would be served. The court may allow an offender to work off the fine by doing community service. If community service work is not available, the misdemeanor shall be punishable by a fine of up to one thousand dollars ($1,000), based on the person's ability to pay.

(d) If an offense specified in this section is committed by a person when he or she is under 21 years of age, but is 13 years of age or older, the court also may suspend the person's driving privilege for one year, pursuant to Section 13202.5 of the Vehicle Code.

529.7. Any person who obtains, or assists another person in obtaining, a driver's license, identification card, vehicle registration certificate, or any other official document issued by the Department of Motor Vehicles, with knowledge that the person obtaining the document is not entitled to the document, is guilty of a misdemeanor, and is punishable by imprisonment in a county jail for up to one year, or a fine of up to one thousand dollars ($1,000), or both.

530. Every person who falsely personates another, in either his private or official capacity, and in such assumed character receives any money or property, knowing that it is intended to be delivered to the individual so personated, with intent to convert the same to his own use, or to that of another person, or to deprive the true owner thereof, is punishable in the same manner and to the same extent as for larceny of the money or property so received.

530.5. (a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), 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, is guilty of a public offense, and upon conviction therefor, shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed one thousand dollars ($1,000), or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed ten thousand dollars ($10,000), or both that imprisonment and fine.

(b) "Personal identifying information," as used in this section, means the name, address, telephone number, health insurance identification number, taxpayer identification number, school identification number, state or federal driver's license number, or identification number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including identification number, address, or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of a person, or an equivalent form of identification.

(c) In any case in which a person willfully obtains personal identifying information of another person, uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

(d) Every person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information, as defined in subdivision (b), of another person is guilty of a public offense, and upon conviction therefor, shall be punished by imprisonment in a county jail not to exceed one year, or a fine not to exceed one thousand dollars ($1,000), or by both that imprisonment and fine.

(e) Every person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information, as defined in subdivision (b), of another person who is deployed to a location outside of the state is guilty of a public offense, and upon conviction therefor, shall be punished by imprisonment in a county jail not to exceed one year, or a fine not to exceed one thousand five hundred dollars ($1,500), or by both that imprisonment and fine.

(f) For purposes of this section, "deployed" means that the person has been ordered to serve temporary military duty during a period when a presidential executive order specifies that the United States is engaged in combat or homeland defense and he or she is either a member of the armed forces, or is a member of the armed forces reserve or the National Guard, who has been called to active duty or active service. It does not include temporary duty for the sole purpose of training or processing or a permanent change of station.

(g) For purposes of this section, "person" means a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity.

530.6. (a) A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another, as described in subdivision (a) of Section 530.5, may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence or place of business, which shall take a police report of the matter, provide the complainant with a copy of that report, and begin an investigation of the facts. If the suspected crime was committed in a different jurisdiction, the local law enforcement agency may refer the matter to the law enforcement agency where the suspected crime was committed for further investigation of the facts.

(b) A person who reasonably believes that he or she is the victim of identity theft may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move, for an expedited judicial determination of his or her factual innocence, where the perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against the perpetrator in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the offense for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly

associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.

(c) After a court has issued a determination of factual innocence pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

(d) A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

(e) The Judicial Council of California shall develop a form for use in issuing an order pursuant to this section.

(f) For purposes of this section, "person" means a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity.

530.8. (a) If a person discovers that an application in his or her name for a loan, credit line or account, credit card, charge card, public utility service, mail receiving or forwarding service, office
or desk space rental service, or commercial mobile radio service has been filed with any person or entity by an unauthorized person, or that an account in his or her name has been opened with a bank, trust company, savings association, credit union, public utility, mail receiving or forwarding service, office or desk space rental service, or commercial mobile radio service provider by an unauthorized person, then, upon presenting to the person or entity with which the
application was filed or the account was opened a copy of a police report prepared pursuant to Section 530.6 and identifying information in the categories of information that the unauthorized person used to complete the application or to open the account, the person, or a law enforcement officer specified by the person, shall be entitled to receive information related to the application or account, including a copy of the unauthorized person's application or application information and a record of transactions or charges associated with the application or account. Upon request by the person in whose name the application was filed or in whose name the account was opened, the person or entity with which the application was filed shall inform him or her of the categories of identifying information that the unauthorized person used to complete the application or to open the account. The person or entity with which the application was
filed or the account was opened shall provide copies of all paper records, records of telephone applications or authorizations, or records of electronic applications or authorizations required by this section, without charge, within 10 business days of receipt of the person's request and submission of the required copy of the police report and identifying information.

(b) Any request made pursuant to subdivision (a) to a person or entity subject to the provisions of Section 2891 of the Public Utilities Code shall be in writing and the requesting person shall be deemed to be the subscriber for purposes of that section.

(c) (1) Before a person or entity provides copies to a law enforcement officer pursuant

to subdivision (a), the person or entity may require the requesting person to submit a signed and dated statement by which the requesting person does all of the following:

(A) Authorizes disclosure for a stated period.

(B) Specifies the name of the agency or department to which the disclosure is authorized.

(C) Identifies the types of records that the requesting person authorizes to be disclosed.

(2) The person or entity shall include in the statement to be signed by the requesting person a notice that the requesting person has the right at any time to revoke the authorization.

(d) (1) A failure to produce records pursuant to subdivision (a) shall be addressed by the court in the jurisdiction in which the victim resides or in which the request for information was issued. At the victim's request, the Attorney General, the district attorney, or the prosecuting city attorney may file a petition to compel the attendance of the person or entity in possession of the records, as described in subdivision (a), and order the production of the requested records to the court. The petition shall contain a declaration from the victim stating when the request for information
was made, that the information requested was not provided, and what response, if any, was made by the person or entity. The petition shall also contain copies of the police report prepared pursuant to Section 530.6 and the request for information made pursuant to this section upon the person or entity in possession of the records, as described in subdivision (a), and these two documents shall be kept confidential by the court. The petition and copies of the police report and the application shall be served upon the person or entity in possession of the records, as described in subdivision (a). The court shall hold a hearing on the petition no later than 10 court
days after the petition is served and filed. The court shall order the release of records to the victim as required pursuant to this section.

(2) In addition to any other civil remedy available, the victim may bring a civil action against the entity for damages, injunctive relief or other equitable relief, and a penalty of one hundred dollars ($100) per day of noncompliance, plus reasonable attorneys' fees.

(e) For the purposes of this section, the following terms have the following meanings:

(1) "Application" means a new application for credit or service, the addition of authorized users to an existing account, the renewal of an existing account, or any other changes made to an existing account.

(2) "Commercial mobile radio service" means "commercial mobile radio service" as defined in Section 20.3 of Title 47 of the Code of Federal Regulations.

(3) "Law enforcement officer" means a peace officer as defined by Section 830.1.

(4) "Person" means a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity.

531. Every person who is a party to any fraudulent conveyance of any lands, tenements, or hereditaments, goods or chattels, or any right or interest issuing out of the same, or to any bond, suit, judgment, or execution, contract or conveyance, had, made, or contrived with intent to deceive and defraud others, or to defeat, hinder, or delay creditors or others of their just debts, damages, or demands; or who, being a party as aforesaid, at any time wittingly and willingly puts in, uses, avows, maintains, justifies, or defends the same, or any of them, as true, and done, had, or made in good faith, or upon good consideration,

or aliens, assigns, or sells any of the lands, tenements, hereditaments, goods, chattels, or other things before mentioned, to him or them conveyed as aforesaid, or any part thereof, is guilty of a misdemeanor.

532. (a) Every person who knowingly and designedly, by any false or fraudulent representation or pretense, defrauds any other person of money, labor, or property, whether real or personal, or who causes or procures others to report falsely of his or her wealth or mercantile character, and by thus imposing upon any person obtains credit, and thereby fraudulently gets possession of money or property, or obtains the labor or service of another, is punishable in the same manner
and to the same extent as for larceny of the money or property so obtained.

(b) Upon a trial for having, with an intent to cheat or defraud another designedly, by any false pretense, obtained the signature of any person to a written instrument, or having obtained from any person any labor, money, or property, whether real or personal, or valuable thing, the defendant cannot be convicted if the false pretense was expressed in language unaccompanied by a false token or writing, unless the pretense, or some note or memorandum thereof is in writing, subscribed by or in the handwriting of the defendant, or unless the pretense is proven by the testimony of two witnesses, or that of one witness and corroborating circumstances. This section does not apply to a prosecution for falsely representing or personating another, and, in that assumed character, marrying, or receiving any money or property.

532a. (1) Any person who shall knowingly make or cause to be made, either directly or indirectly or through any agency whatsoever, any false statement in writing, with intent that it shall be relied upon, respecting the financial condition, or means or ability to pay, of himself, or any other person, firm or corporation, in whom he is interested, or for whom he is acting, for the purpose of procuring in any form whatsoever, either the delivery of personal property, the payment of cash, the making of a loan or credit, the extension of a credit, the execution of a contract of guaranty or suretyship, the discount of an account receivable, or the making, acceptance, discount, sale or indorsement of a bill of exchange, or promissory note, for the benefit of either himself or of such person, firm or corporation shall be guilty of a public offense.

(2) Any person who knowing that a false statement in writing has been made, respecting the financial condition or means or ability to pay, of himself, or a person, firm or corporation in which he is interested, or for whom he is acting, procures, upon the faith thereof, for the benefit either of himself, or of such person, firm or corporation, either or any of the things of benefit mentioned in the first subdivision of this section shall be guilty of a public offense.

(3) Any person who knowing that a statement in writing has been made, respecting the financial condition or means or ability to pay of himself or a person, firm or corporation, in which he is interested, or for whom he is acting, represents on a later day in writing that the statement theretofore made, if then again made on said day, would be then true, when in fact, said statement if then made would be false, and procures upon the faith thereof, for the benefit either of himself or of such person, firm or corporation either or any of the things of benefit mentioned in the first subdivision of this section shall be guilty of a public offense.

(4) Any person committing a public offense under subdivision (1), (2), or (3) shall be

guilty of a misdemeanor, punishable by a fine of not more than one thousand dollars ($1,000), or by imprisonment in the county jail for not more than six months, or by both such fine and imprisonment. Any person who violates the provisions of subdivision (1), (2), or (3), by using a fictitious name, social security number, business name, or business address, or by falsely representing himself or herself to be another person or another business, is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000) or by imprisonment in the state prison, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500) or by imprisonment in the county jail not exceeding one year, or by both
such fine and imprisonment.

(5) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

532b. (a) Any person who falsely represents himself or herself as a veteran or ex-serviceman of any war in which the United States was engaged, in connection with the soliciting of aid or the sale or attempted sale of any property, is guilty of a misdemeanor.

(b) Any person who falsely claims, or presents himself or herself, to be a veteran or member of the Armed Forces of the United States, with the intent to defraud, is guilty of a misdemeanor.

(c) This section does not apply to face-to-face solicitations involving less than ten dollars ($10).

538d. (a) Any person other than one who by law is given the authority of a peace officer, who willfully wears, exhibits, or uses the authorized uniform, insignia, emblem, device, label, certificate, card, or writing, of a peace officer, with the intent of fraudulently impersonating a peace officer, or of fraudulently inducing the belief that he or she is a peace officer, is guilty of a misdemeanor.

(b) (1) Any person, other than the one who by law is given the authority of a peace officer, who willfully wears, exhibits, or uses the badge of a peace officer with the intent of fraudulently impersonating a peace officer, or of fraudulently inducing the belief that he or she is a peace officer, is guilty of a misdemeanor punishable by imprisonment in a county jail not to exceed one year, by a fine not to exceed two thousand dollars ($2,000), or by both that imprisonment and fine.

(2) Any person who willfully wears or uses any badge that falsely purports to be authorized for the use of one who by law is given the authority of a peace officer, or which so resembles the authorized badge of a peace officer as would deceive any ordinary reasonable person into believing that it is authorized for the use of one who by law is given the authority of a peace officer, for the purpose of fraudulently impersonating a peace officer, or of fraudulently inducing the belief that he or she is a peace officer, is guilty of a misdemeanor punishable by imprisonment in a county jail not to exceed one year, by a fine not to exceed two thousand dollars ($2,000), or by both that imprisonment and fine.

(c) Any person who willfully wears, exhibits, or uses, or who willfully makes, sells, loans, gives, or transfers to another, any badge, insignia, emblem, device, or any label, certificate, card, or writing, which falsely purports to be authorized for the use of one who by law is given the authority of a peace officer, or which so resembles the authorized badge, insignia, emblem, device, label, certificate, card, or writing of a peace

officer as would deceive an ordinary reasonable person into believing that it is authorized for the use of one who by law is given the authority of a peace officer, is guilty of a misdemeanor, except that any person who makes or sells any badge under the circumstances described in this subdivision is subject to a fine not to exceed fifteen thousand dollars ($15,000).

2.2.2. *Civil Code*

1725. (a) Unless permitted under subdivision (c), no person accepting a negotiable instrument as payment in full or in part for goods or services sold or leased at retail shall do any of the following:

(1) Require the person paying with a negotiable instrument to provide a credit card as a condition of acceptance of the negotiable instrument, or record the number of the credit card.

(2) Require, as a condition of acceptance of the negotiable instrument, or cause the person paying with a negotiable instrument to sign a statement agreeing to allow his or her credit card to be charged to cover the negotiable instrument if returned as no good.

(3) Record a credit card number in connection with any part of the transaction described in this subdivision.

(4) Contact a credit card issuer to determine if the amount of any credit available to the person paying with a negotiable instrument will cover the amount of the negotiable instrument.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Check guarantee card" means a card issued by a financial institution, evidencing an agreement under which the financial institution will not dishonor a check drawn upon itself, under the terms and conditions of the agreement.

(2) "Credit card" has the meaning specified in Section 1747.02, and does not include a check guarantee card or a card that is both a credit card and a check guarantee card.

(3) "Negotiable instrument" has the meaning specified in Section 3104 of the Commercial Code.

(4) "Retail" means a transaction involving the sale or lease of goods or services or both, between an individual, corporation, or other entity regularly engaged in business and a consumer, for use by the consumer and not for resale.

(c) This section does not prohibit any person from doing any of the following:

(1) Requiring the production of reasonable forms of positive identification, other than a credit card, which may include a driver's license or a California state

identification card, or where one of these is not available, another form of photo identification, as a condition of acceptance of a negotiable instrument.

(2) Requesting, but not requiring, a purchaser to voluntarily display a credit card as an indicia of creditworthiness or financial responsibility, or as an additional identification, provided the only information concerning the credit card which is recorded is the type of credit card displayed, the issuer of the card, and the expiration date of the card. All retailers that request the display of a credit card pursuant to this paragraph shall inform the customer, by either of the following methods, that displaying the credit card is not a requirement for check writing:

(A) By posting the following notice in a conspicuous location in the unobstructed view of the public within the premises where the check is being written, clearly and legibly: "Check writing ID: credit card may be requested but not required for purchases."

(B) By training and requiring the sales clerks or retail employees requesting the credit card to inform all check writing customers that they are not required to display a credit card to write a check.

(3) Requesting production of, or recording, a credit card number as a condition for cashing a negotiable instrument that is being used solely to receive cash back from the person.

(4) Requesting, receiving, or recording a credit card number in lieu of requiring a deposit to secure payment in event of default, loss, damage, or other occurrence.

(5) Requiring, verifying, and recording the purchaser's name, address, and telephone number.

(6) Requesting or recording a credit card number on a negotiable instrument used to make a payment on that credit card account.

(d) This section does not require acceptance of a negotiable instrument whether or not a credit card is presented.

(e) Any person who violates this section is subject to a civil penalty not to exceed two hundred fifty dollars ($250) for a first violation, and to a civil penalty not to exceed one thousand dollars ($1,000) for a second or subsequent violation, to be assessed and collected in a civil action brought by the person paying with a negotiable instrument, by the Attorney General, or by the district attorney or city attorney of the county or city in which the violation occurred. However, no civil penalty shall be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid such an error. When collected, the civil penalty shall be payable, as appropriate, to the person paying with a negotiable instrument who brought the action or to the general fund of whichever governmental entity brought the action to assess the civil penalty.

(f) The Attorney General, or any district attorney or city attorney within his or her

respective jurisdiction, may bring an action in the superior court in the name of the people of the State of California to enjoin violation of subdivision (a) and, upon notice to the defendant of not less than five days, to temporarily restrain and enjoin the violation. If it appears to the satisfaction of the court that the defendant has, in fact, violated subdivision (a), the court may issue an injunction restraining further violations, without requiring proof that any person has been damaged by the violation. In these proceedings, if the court finds that the defendant has violated subdivision (a), the court may direct the defendant to pay any or all costs incurred by the Attorney General, district attorney, or city attorney in seeking or obtaining injunctive relief pursuant to this subdivision.

(g) Actions for collection of civil penalties under subdivision (e) and for injunctive relief under subdivision (f) may be consolidated.

1747.06. (a) A credit card issuer that mails an offer or solicitation to receive a credit card and, in response, receives a completed application for a credit card that lists an address that is different from the address on the offer or solicitation shall verify the change of address by contacting the person to whom the solicitation or offer was mailed.

(b) Notwithstanding any other provision of law, a person to whom an offer or solicitation to receive a credit card is made shall not be liable for the unauthorized use of a credit card issued in response to that offer or solicitation if the credit card issuer does not verify the change of address pursuant to subdivision (a) prior to the issuance of the credit card, unless the credit card issuer proves that this person actually incurred the charge on the credit card.

(c) When a credit card issuer receives a written or oral request for a change of the cardholder's billing address and then receives a written or oral request for an additional credit card within 10 days after the requested address change, the credit card issuer shall not mail the requested additional credit card to the new address or, alternatively, activate the requested additional credit card, unless the credit card issuer has verified the change of address.

(d) This section shall become operative on July 1, 2000.

1747.08. (a) Except as provided in subdivision (c), no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following:

(1) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise.

(2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the

credit card transaction form or otherwise.

(3) Utilize, in any credit card transaction, a credit card form which contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder.

(b) For purposes of this section "personal identification information," means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number.

(c) Subdivision (a) does not apply in the following instances:

(1) If the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar occurrence.

(2) Cash advance transactions.

(3) If the person, firm, partnership, association, or corporation accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction or is obligated to collect and record the personal identification information by federal law or regulation.

(4) If personal identification information is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders.

(d) This section does not prohibit any person, firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction form or otherwise.

(e) Any person who violates this section shall be subject to a civil penalty not to exceed two hundred fifty dollars ($250) for the first violation and one thousand dollars ($1,000) for each subsequent violation, to be assessed and collected in a civil action brought by the person paying with a credit card, by the Attorney General, or by the district attorney or city attorney of the county or city in which the violation occurred. However, no civil penalty shall be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid that error. When collected, the civil penalty shall be payable, as appropriate, to the person paying with a credit card who brought the action, or to the general fund of whichever governmental entity brought the action to assess the civil penalty.

(f) The Attorney General, or any district attorney or city attorney within his or her respective jurisdiction, may bring an action in the superior court in the name of the people of the State of California to enjoin violation of subdivision (a) and, upon notice to the defendant of not less than five days, to temporarily restrain and enjoin the violation. If it appears to the satisfaction of the court that the defendant has, in fact, violated subdivision (a), the court may issue an injunction restraining further violations, without requiring proof that any person has been damaged by the violation. In these proceedings, if the court finds that the defendant has violated subdivision (a), the court may direct the defendant to pay any or all costs incurred by the Attorney General, district attorney, or city attorney in seeking or obtaining injunctive relief pursuant to this subdivision.

(g) Actions for collection of civil penalties under subdivision (e) and for injunctive relief under subdivision (f) may be consolidated.

(h) The changes made to this section by Chapter 458 of the Statutes of 1995 apply only to credit card transactions entered into on and after January 1, 1996. Nothing in those changes shall be construed to affect any civil action which was filed before January 1, 1996.

1747.09. (a) Except as provided in this section, no person, firm, partnership, association, corporation, or limited liability company that accepts credit or debit cards for the transaction of business shall print more than the last five digits of the credit or debit card account number or the expiration date upon any of the following:

(1) Any receipt provided to the cardholder.

(2) Any receipt retained by the person, firm, partnership, association, corporation, or limited liability company, which is printed at the time of the purchase, exchange, refund, or return, and is signed by the cardholder.

(3) Any receipt retained by the person, firm, partnership, association, corporation, or limited liability company, which is printed at the time of the purchase, exchange, refund, or return, but is not signed by the cardholder, because the cardholder used a personal identification number to complete the transaction.

(b) This section shall apply only to receipts that include a credit or debit card account number that are electronically printed and shall not apply to transactions in which the sole means of recording the person's credit or debit card account number is by handwriting or by an imprint or copy of the credit or debit card.

(c) This section shall not apply to documents, other than the receipts described in paragraphs (1) to (3), inclusive, of subdivision (a), used for internal administrative purposes.

(d) Paragraphs (2) and (3) of subdivision (a) shall become operative on January 1, 2009.

1798.79.8. For purposes of this title:

(a) "Person or entity" means any individual, corporation, partnership, joint venture, or any business entity, or any state or local agency.

(b) "Personally identifying information" means:

(1) First and last name or last name only.

(2) Home or other physical address, including, but not limited to, a street name or ZIP Code, other than an address obtained pursuant to the California Safe At Home program or a business mailing address for the victim service provider.

(3) Electronic mail address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's electronic mail address.

(4) Telephone number, other than a business telephone number for the victim service provider.

(5) Social security number.

(6) Date of birth, with the exception of the year of birth.

(7) Internet protocol address or host name that identifies an individual.

(8) Any other information, including, but not limited to, the first and last names of children and relatives, racial or ethnic background, or religious affiliation, that, in combination with any other nonpersonally identifying information, would serve to identify any individual.

(c) "Victim service provider" means a nongovernmental organization or entity that provides shelter, programs, or services at low cost, no cost, or on a sliding scale to victims of domestic violence, dating violence, sexual assault, or stalking, or their children, either directly or through other contractual arrangements, including rape crisis centers, domestic violence shelters, domestic violence transitional housing programs, and other programs with the primary mission to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, or their children, whether or not that program exists in an agency that provides additional services.

1785.10. (a) Every consumer credit reporting agency shall, upon request and proper identification of any consumer, allow the consumer to visually inspect all files maintained regarding that consumer at the time of the request.

(b) Every consumer reporting agency, upon contact by a consumer by telephone, mail, or in person regarding information which may be contained in the agency files regarding that consumer, shall promptly advise the consumer of his or her rights under Sections 1785.11.8, 1785.19, and 1785.19.5, and of the obligation of the agency to

provide disclosure of the files in person, by mail, or by telephone pursuant to Section 1785.15, including the obligation of the agency to provide a decoded written version of the file or a written copy of the file with an explanation of any code, including any credit score used, and the key factors, as defined in Section 1785.15.1, if the consumer so requests that copy. The disclosure shall be provided in the manner selected by the consumer, chosen from among any reasonable means available to the consumer credit reporting agency. The agency shall determine the applicability of subdivision (1) of Section 1785.17 and, where applicable, the agency shall inform the consumer of the rights under that section.

(c) All information on a consumer in the files of a consumer credit reporting agency at the time of a request for inspection under subdivision (a), shall be available for inspection, including the names, addresses and, if provided by the sources of information, the telephone numbers identified for customer service for the sources of information.

(d) (1) The consumer credit reporting agency shall also disclose the recipients of any consumer credit report on the consumer which the consumer credit reporting agency has furnished:

(A) For employment purposes within the two-year period preceding the request.

(B) For any other purpose within the 12-month period preceding the request.

(2) Disclosure of recipients of consumer credit reports for purposes of this subdivision shall include the name of the recipient or, if applicable, the fictitious business name under which the recipient does business disclosed in full. The identification shall also include the address and, if provided by the recipient, the telephone number identified for customer service for the recipient.

(e) The consumer credit reporting agency shall also disclose a record of all inquiries received by the agency in the 12-month period preceding the request that identified the consumer in connection with a credit transaction which is not initiated by the consumer. This record of inquiries shall include the name, address and, if provided by the recipient, the telephone number identified for customer service for each recipient making an inquiry.

(f) Any consumer credit reporting agency when it is subject to the provisions of Section 1785.22 is exempted from the requirements of subdivisions (c), (d), and (e), only with regard to the provision of the address and telephone number.

(g) Any consumer credit reporting agency, that provides a consumer credit report to another consumer credit reporting agency that procures the consumer credit report for the purpose of resale and is subject to Section 1785.22, is exempted from the requirements of subdivisions (d) and (e), only with regard to the provision of the address and telephone number regarding each prospective user to which the consumer credit report was sold.

(h) This section shall become operative on January 1, 2003.

1785.11. (a) A consumer credit reporting agency shall furnish a consumer credit report only under the following circumstances:

(1) In response to the order of a court having jurisdiction to issue an order.

(2) In accordance with the written instructions of the consumer to whom it relates.

(3) To a person whom it has reason to believe:

(A) Intends to use the information in connection with a credit transaction, or entering or enforcing an order of a court of competent jurisdiction for support, involving the consumer as to whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

(B) Intends to use the information for employment purposes; or

(C) Intends to use the information in connection with the underwriting of insurance involving the consumer, or for insurance claims settlements; or

(D) Intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider the applicant's financial responsibility or status; or

(E) Intends to use the information in connection with the hiring of a dwelling unit, as defined in subdivision (c) of Section 1940; or

(F) Otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

(b) A consumer credit reporting agency may furnish information for purposes of a credit transaction specified in subparagraph (A) of paragraph (3) of subdivision (a), where it is a credit transaction that is not initiated by the consumer, only under the circumstances specified in paragraph (1) or (2), as follows:

(1) The consumer authorizes the consumer credit reporting agency to furnish the consumer credit report to the person.

(2) The proposed transaction involves a firm offer of credit to the consumer, the consumer credit reporting agency has complied with subdivision (d), and the consumer has not elected pursuant to paragraph (1) of subdivision (d) to have the consumer's name excluded from lists of names provided by the consumer credit reporting agency for purposes of reporting in connection with the potential issuance of firm offers of credit. A consumer credit reporting agency may provide only the following information pursuant to this paragraph:

(A) The name and address of the consumer.

(B) Information pertaining to a consumer that is not identified or identifiable with a particular consumer.

(c) Except as provided in paragraph (3) of subdivision (a) of Section 1785.15, a consumer credit reporting agency shall not furnish to any person a record of inquiries solely resulting from credit transactions that are not initiated by the consumer.

(d) (1) A consumer may elect to have his or her name and address excluded from any list provided by a consumer credit reporting agency pursuant to paragraph (2) of subdivision (b) by notifying the consumer credit reporting agency, by telephone or in writing, through the notification system maintained by the consumer credit reporting agency pursuant to subdivision (e), that the consumer does not consent to any use of consumer credit reports relating to the consumer in connection with any transaction that is not initiated by the consumer.

(2) An election of a consumer under paragraph (1) shall be effective with respect to a consumer credit reporting agency, and any affiliate of the consumer credit reporting agency, on the date on which the consumer notifies the consumer credit reporting agency.

(3) An election of a consumer under paragraph (1) shall terminate and be of no force or effect following notice from the consumer to the consumer credit reporting agency, through the system established pursuant to subdivision (e), that the election is no longer effective.

(e) Each consumer credit reporting agency that furnishes a prequalifying report pursuant to subdivision (b) in connection with a credit transaction not initiated by the consumer shall establish and maintain a notification system, including a toll-free telephone number, that permits any consumer, with appropriate identification and for which the consumer credit reporting agency has a file, to notify the consumer credit reporting agency of the consumer's election to have the consumer's name removed from any list of names and addresses provided by the consumer credit reporting agency, and by any affiliated consumer credit reporting agency, pursuant to paragraph (2) of subdivision (b). Compliance with the requirements of this subdivision by a consumer credit reporting agency shall constitute compliance with those requirements by any affiliate of that consumer credit reporting agency.

(f) Each consumer credit reporting agency that compiles and maintains files on consumers on a nationwide basis shall establish and maintain a notification system under paragraph (1) of subdivision (e) jointly with its affiliated consumer credit reporting agencies.

1785.11.1. (a) A consumer may elect to place a security alert in his or her credit report by making a request in writing or by telephone to a consumer credit reporting agency. "Security alert" means a notice placed in a consumer's credit report, at the request of the consumer, that notifies a recipient of the credit report that the consumer's identity may have been used without the consumer's consent to fraudulently obtain goods or services in the consumer's name.

(b) A consumer credit reporting agency shall notify each person requesting consumer credit information with respect to a consumer of the existence of a security alert in the credit report of that consumer, regardless of whether a full credit report, credit

score, or summary report is requested.

(c) Each consumer credit reporting agency shall maintain a toll-free telephone number to accept security alert requests from consumers 24 hours a day, seven days a week.

(d) The toll-free telephone number shall be included in any written disclosure by a consumer credit reporting agency to any consumer pursuant to Section 1785.15 and shall be printed in a clear and conspicuous manner.

(e) A consumer credit reporting agency shall place a security alert on a consumer's credit report no later than five business days after receiving a request from the consumer.

(f) The security alert shall remain in place for at least 90 days, and a consumer shall have the right to request a renewal of the security alert.

(g) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, or with the purchase, lease, or rental of goods or non-credit-related services and who receives notification of a security alert pursuant to subdivision (a) may not lend money, extend credit, or complete the purchase, lease, or rental of goods or non-credit-related services without taking reasonable steps to verify the consumer's identity, in order to ensure that the application for an extension of credit or for the purchase, lease, or rental of goods or non-credit-related services is not the result of identity theft. If the consumer has placed a statement with the security alert in his or her file requesting that identity be verified by calling a specified telephone number, any person who receives that statement with the security alert in a consumer's file pursuant to subdivision (a) shall take reasonable steps to verify the identity of the consumer by contacting the consumer using the specified telephone number prior to lending money, extending credit, or completing the purchase, lease, or rental of goods or non-credit-related services. If a person uses a consumer credit report to facilitate the extension of credit or for another permissible purpose on behalf of a subsidiary, affiliate, agent, assignee, or prospective assignee, that person may verify a consumer's identity under this section in lieu of the subsidiary, affiliate, agent, assignee, or prospective assignee.

(h) For purposes of this section, "extension of credit" does not include an increase in the dollar limit of an existing open-end credit plan, as defined in Regulation Z issued by the Board of Governors of the Federal Reserve System (12 C.F.R. 226.2), or any change to, or review of, an existing credit account.

(i) If reasonable steps are taken to verify the identity of the consumer pursuant to subdivision (b) of Section 1785.20.3, those steps constitute compliance with the requirements of this section, except that if a consumer has placed a statement including a telephone number with the security alert in his or her file, his or her identity shall be verified by contacting the consumer using that telephone number as specified pursuant to subdivision (g).

(j) A consumer credit reporting agency shall notify each consumer who has requested that a security alert be placed on his or her consumer credit report of the

expiration date of the alert.

(k) Notwithstanding Section 1785.19, any consumer credit reporting agency that recklessly, willfully, or intentionally fails to place a security alert pursuant to this section shall be liable for a penalty in an amount of up to two thousand five hundred dollars ($2,500) and reasonable attorneys' fees.

1785.11.2. (a) A consumer may elect to 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. "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 not be released to a third party without prior express authorization from the consumer. This subdivision 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.

(b) A consumer credit reporting agency shall place a security freeze on a consumer's credit report no later than five business days after receiving a written request from the consumer.

(c) The consumer credit reporting agency shall send a written confirmation of the security freeze to the consumer within 10 business days and shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit for a specific party or period of time.

(d) If the consumer wishes to allow his or her credit report to be accessed for a specific party 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 the following:

(1) Proper identification, as defined in subdivision (c) of Section 1785.15.

(2) The unique personal identification number or password provided by the credit reporting agency pursuant to subdivision (c).

(3) The proper information regarding the third party who is to receive the credit report or the time period for which the report shall be available to users of the credit report.

(e) A consumer credit reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to subdivision (d), shall comply with the request no later than three business days after receiving the request.

(f) A consumer credit reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a credit report pursuant to subdivision (d) in an expedited manner.

(g) A consumer credit reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:

(1) Upon consumer request, pursuant to subdivision (d) or (j).

(2) If the consumer's credit report was frozen due to a material misrepresentation of

fact by the consumer. If a consumer credit reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this paragraph, the consumer credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(h) If a third party requests access to a consumer credit report n which a security freeze is in effect, and this request is in connection with an application for credit or any other use, and the consumer does not allow his or her credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze, the consumer credit reporting agency shall disclose the process of placing and temporarily lifting a freeze, and the process for allowing access to information from the consumer's credit report for a specific party or period of time while the freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer credit reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides both of the following:

(1) Proper identification, as defined in subdivision (c) of Section 1785.15.

(2) The unique personal identification number or password provided by the credit reporting agency pursuant to subdivision (c).

(k) A consumer credit reporting agency shall require proper identification, as defined in subdivision (c) of Section 1785.15, of the person making a request to place or remove a security freeze.

(l) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

(1) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee
of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument. For purposes of this paragraph, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subdivision (d) of Section 1785.11.2 for purposes of facilitating the extension of credit or other permissible use.

(3) Any state or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, or subpoena.

(4) A child support agency acting pursuant to Chapter 2 of Division 17 of the Family Code or Title IV-D of the Social Security Act (42 U.S.C. et seq.).

(5) The State Department of Health Services or its agents or assigns acting to investigate Medi-Cal fraud.

(6) The Franchise Tax Board or its agents or assigns acting to investigate or collect

delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities.

(7) The use of credit information for the purposes of prescreening as provided for by the federal Fair Credit Reporting Act.

(8) Any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed.

(9) Any person or entity for the purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.

(m) This act does not prevent a consumer credit reporting agency from charging a fee of no more than ten dollars ($10) to a consumer for each freeze, removal of the freeze, or temporary lift of the freeze for a period of time, or a fee of no more than twelve dollars ($12) for a temporary lift of a freeze for a specific party, regarding access to a consumer credit report, except that a consumer credit reporting agency may not charge a fee to a victim of identity theft who has submitted a valid police report or valid Department of Motor Vehicles investigative report that alleges a violation of Section 530.5 of the Penal Code.

1785.11.3. (a) If a security freeze is in place, a consumer credit reporting agency shall not change any of the following official information in a consumer 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: name, date of birth, social security number, and address. Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and to the former address.

(b) If a consumer has placed a security alert, a consumer credit reporting agency shall provide the consumer, upon request, with a free copy of his or her credit report at the time the 90-day security alert period expires.

1785.11.4. The provisions of Sections 1785.11.1, 1785.11.2, and 1785.11.3 do not apply to a consumer credit reporting agency that acts only as a reseller of credit information pursuant to Section 1785.22 by assembling and merging information contained in the data base of another consumer credit reporting agency or multiple consumer credit reporting agencies, and does not maintain a permanent data base of credit information from which new consumer credit reports are produced. However, a consumer credit reporting agency acting pursuant to Section 1785.22 shall honor any security freeze placed on a consumer credit report by another consumer credit reporting agency.

1785.11.8. A consumer may elect that his or her name shall be removed from any list that a consumer credit reporting agency furnishes for credit card solicitations, by notifying the consumer credit reporting agency, by telephone or in writing, pursuant to the notification system maintained by the consumer credit reporting agency pursuant to subdivision (d) of Section 1785.11. The election shall be effective for a minimum of two years, unless otherwise specified by the consumer.

1785.14. (a) Every consumer credit reporting agency shall maintain reasonable procedures designed to avoid violations of Section 1785.13 and to limit furnishing of consumer credit reports to the purposes listed under Section 1785.11. These procedures

shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought and certify that the information will be used for no other purposes. From the effective date of this act the consumer credit reporting agency shall keep a record of the purposes as stated by the user. Every consumer credit reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by the prospective user prior to furnishing the user a consumer report. No consumer credit reporting agency may furnish a consumer credit report to any person unless the consumer credit reporting agency has reasonable grounds for believing that the consumer credit report will be used by the person for the purposes listed in Section 1785.11. A consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will be used by the person for the purposes listed in Section 1785.11 unless all of the following requirements are met:

(1) If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name.

(2) If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller certifies, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail.

(3) If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed.

(b) Whenever a consumer credit reporting agency prepares a consumer credit report, it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates. These reasonable procedures shall include, but not be limited to, permanent retention by the consumer credit reporting agency in the consumer's file, or a separately individualized file, of that portion of the data in the file that is used by the consumer credit reporting agency to identify the individual consumer pursuant to paragraph (1) of subdivision (a). This permanently retained data shall be available for use in either a reinvestigation pursuant to subdivision (a) of Section 1785.16, an investigation where the consumer has filed a police report pursuant to subdivision (k) of Section 1785.16, or a restoration of a file involving the consumer. If the permanently retained identifying information is retained in a consumer's file, it shall be clearly identified in the file in order for an individual who reviews the file to easily distinguish between the permanently stored identifying

information and any other identifying information that may be a part of the file. This retention requirement shall not apply to data that is reported in error, that is obsolete, or that is found to be inaccurate through the results of a reinvestigation initiated by a consumer pursuant to subdivision (a) of Section 1785.16.

(c) No consumer credit reporting agency may prohibit any user of any consumer credit report furnished by the consumer credit reporting agency from disclosing the contents of the consumer credit report to the consumer who is the subject of the report if adverse action may be taken by the user based in whole or in part on the consumer credit report. The act of disclosure to the consumer by the user of the contents of a consumer credit report shall not be a basis for liability of the consumer credit reporting agency or the user under Section 1785.31.

(d) A consumer credit reporting agency shall provide a written notice to any person who regularly and in the ordinary course of business supplies information to the consumer credit reporting agency concerning any consumer or to whom a consumer credit report is provided by the consumer credit reporting agency. The notice shall specify the person's obligations under this title. Copies of the appropriate code sections shall satisfy the requirement of this subdivision.

1785.15.3. (a) In addition to any other rights the consumer may have under this title, every consumer credit reporting agency, after being contacted by telephone, mail, or in person by any consumer who has reason to believe he or she may be a victim of identity theft, shall promptly provide to that consumer a statement, written in a clear and conspicuous manner, describing the statutory rights of victims of identity theft under this title.

(b) Every consumer credit reporting agency shall, upon the receipt from a victim of identity theft of a police report prepared pursuant to Section 530.6 of the Penal Code, or a valid investigative report made by a Department of Motor Vehicles investigator with peace officer status regarding the public offenses described in Section 530.5 of the Penal Code, provide the victim, free of charge and upon request, with up to 12 copies of his or her file during a consecutive 12-month period, not to exceed one copy per month, following the date of the police report. Notwithstanding any other provision of this title, the maximum number of free reports a victim of identity theft is entitled to obtain under this title is 12 per year, as provided by this subdivision.

(c) Subdivision (a) does not apply to a consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer reporting agency or agencies and that does not maintain a permanent database of credit information from which new credit reports are produced.

(d) The provisions of this section shall become effective July 1, 2003.

1785.16. (a) If the completeness or accuracy of any item of information contained in his or her file is disputed by a consumer, and the dispute is conveyed directly to the consumer credit reporting agency by the consumer or user on behalf of the consumer, the consumer credit reporting agency shall within a reasonable period of time and without charge, reinvestigate and record the current status of the disputed information before the end of the 30-business-day period beginning on the date the agency receives notice of the dispute from the consumer or user, unless the consumer credit reporting agency has reasonable grounds to believe and determines that the dispute by the consumer is

frivolous or irrelevant, including by reason of a failure of the consumer to provide sufficient information, as requested by the consumer credit reporting agency, to investigate the dispute. Unless the consumer credit reporting agency determines that the dispute is frivolous or irrelevant, before the end of the five-business-day period beginning on the date the consumer credit reporting agency receives notice of dispute under this section, the agency shall notify any person who provided information in dispute at the address and in the manner specified by the person. A consumer credit reporting agency may require that disputes by consumers be in writing.

(b) In conducting that reinvestigation the consumer credit reporting agency shall review and consider all relevant information submitted by the consumer with respect to the disputed item of information. If the consumer credit reporting agency determines that the dispute is frivolous or irrelevant, it shall notify the consumer by mail or, if authorized by the consumer for that purpose, by any other means available to the consumer credit reporting agency, within five business days after that determination is made that it is terminating its reinvestigation of the item of information. In this notification, the consumer credit reporting agency shall state the specific reasons why it has determined that the consumer's dispute is frivolous or irrelevant. If the disputed item of information is found to be inaccurate, missing, or can no longer be verified by the evidence submitted, the consumer credit reporting agency shall promptly add, correct, or delete that information from the consumer's file.

(c) No information may be reinserted in a consumer's file after having been deleted pursuant to this section unless the person who furnished the information certifies that the information is accurate.

If any information deleted from a consumer's file is reinserted in the file, the consumer credit reporting agency shall promptly notify the consumer of the reinsertion in writing or, if authorized by the consumer for that purpose, by any other means available to the consumer credit reporting agency. As part of, or in addition to, this notice the consumer credit reporting agency shall, within five business days of reinserting the information, provide the consumer in writing (1) a statement that the disputed information has been reinserted, (2) a notice that the agency will provide to the consumer, within 15 days following a request, the name, address, and telephone number of any furnisher of information contacted or which contacted the consumer credit reporting agency in connection with the reinsertion, (3) the toll-free telephone number of the consumer credit reporting agency that the consumer can use to obtain this name, address, and telephone number, and (4) a notice that the consumer has the right to a reinvestigation of the information reinserted by the consumer credit reporting agency and to add a statement to his or her file disputing the accuracy or completeness of the information.

(d) A consumer credit reporting agency shall provide written notice to the consumer of the results of any reinvestigation under this subdivision, within five days of completion of the reinvestigation. The notice shall include (1) a statement that the reinvestigation is completed, (2) a consumer credit report that is based on the consumer's file as that file is revised as a result of the reinvestigation, (3) a description or indication of any changes made in the consumer credit report as a result of those revisions to the consumer's file and a description of any changes made or sought by the consumer that were not made and an explanation why they were not made, (4) a notice that, if requested by the

consumer, a description of the procedure used to determine the accuracy and completeness of the information shall be provided to the consumer by the consumer credit reporting agency, including the name, business address, and telephone number of any furnisher of information contacted in connection with that information, (5) a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the information, (6) a notice that the consumer has the right to request that the consumer credit reporting agency furnish notifications under subdivision (h), (7) a notice that the dispute will remain on file with the agency as long as the credit information is used, and (8) a statement about the details of the dispute will be furnished to any recipient as long as the credit information is retained in the agency's data base. A consumer credit reporting agency shall provide the notice pursuant to this subdivision respecting the procedure used to determine the accuracy and completeness of information, not later than 15 days after receiving a request from the consumer.

(e) The presence of information in the consumer's file that contradicts the contention of the consumer shall not, in and of itself, constitute reasonable grounds for believing the dispute is frivolous or irrelevant.

(f) If the consumer credit reporting agency determines that the dispute is frivolous or irrelevant, or if the reinvestigation does not resolve the dispute, or if the information is reinserted into the consumer's file pursuant to subdivision (c), the consumer may file a brief statement setting forth the nature of the dispute. The consumer credit reporting agency may limit these statements to not more than 100 words if it provides the consumer with assistance in writing a clear summary of the dispute.

(g) Whenever a statement of dispute is filed, the consumer credit reporting agency shall, in any subsequent consumer credit report containing the information in question, clearly note that the information is disputed by the consumer and shall include in the report either the consumer's statement or a clear and accurate summary thereof.

(h) Following the deletion of information from a consumer's file pursuant to this section, or following the filing of a statement of dispute pursuant to subdivision (f), the consumer credit reporting agency, at the request of the consumer, shall furnish notification that the item of information has been deleted or that the item of information is disputed. In the case of disputed information, the notification shall include the statement or summary of the dispute filed pursuant to subdivision (f). This notification shall be furnished to any person designated by the consumer who has, within two years prior to the deletion or the filing of the dispute, received a consumer credit report concerning the consumer for employment purposes, or who has, within 12 months of the deletion or the filing of the dispute, received a consumer credit report concerning the consumer for any other purpose, if these consumer credit reports contained the deleted or disputed information. The consumer credit reporting agency shall clearly and conspicuously disclose to the consumer his or her rights to make a request for this notification. The disclosure shall be made at or prior to the time the information is deleted pursuant to this section or the consumer's statement regarding the disputed information is received pursuant to subdivision (f).

(i) A consumer credit reporting agency shall maintain reasonable procedures to prevent the reappearance in a consumer's file and in consumer credit reports of information that has been deleted pursuant to this section and not reinserted pursuant to subdivision (c).

(j) If the consumer's dispute is resolved by deletion of the disputed information within three business days, beginning with the day the consumer credit reporting agency receives notice of the dispute in accordance with subdivision (a), and provided that verification thereof is provided to the consumer in writing within five business days following the deletion, then the consumer credit reporting agency shall be exempt from requirements for further action under subdivisions (d), (f), and (g).

(k) If a consumer submits to a credit reporting agency a copy of a valid police report, or a valid investigative report made by a Department of Motor Vehicles investigator with peace officer status, filed pursuant to Section 530.5 of the Penal Code, the consumer credit reporting agency shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of Section 530.5 of the Penal Code so that the information cannot be reported. The consumer credit reporting agency shall promptly notify the furnisher of the information that the information has been so blocked. Furnishers of information and consumer credit reporting agencies shall ensure that information is unblocked only upon a preponderance of the evidence establishing the facts required under paragraph (1), (2), or (3). The permanently blocked information shall be unblocked only if: (1) the information was blocked due to a material misrepresentation of fact by the consumer or fraud, or (2) the consumer agrees that the blocked information, or portions of the blocked information, were blocked in error, or (3) the consumer knowingly obtained possession of goods, services, or moneys as a result of the blocked transaction or transactions or the consumer should have known that he or she obtained possession of goods, services, or moneys as a result of the blocked transaction or transactions. If blocked information is unblocked pursuant to this subdivision, the consumer shall be promptly notified in the same manner as consumers are notified of the reinsertion of information pursuant to subdivision (c). The prior presence of the blocked information in the consumer credit reporting agency's file on the consumer is not evidence of whether the consumer knew or should have known that he or she obtained possession of any goods, services, or moneys. For the purposes of this subdivision, fraud may be demonstrated by circumstantial evidence. In unblocking information pursuant to this subdivision, furnishers and consumer credit reporting agencies shall be subject to their respective requirements pursuant to this title regarding the completeness and accuracy of information.

(l) In unblocking information as described in subdivision (k), a consumer reporting agency shall comply with all requirements of this section and 15 U.S.C. Sec. 1681i relating to reinvestigating disputed information. In addition, a consumer reporting agency shall accept the consumer's version of the disputed information and correct or delete the disputed item when the consumer submits to the consumer reporting agency documentation obtained from the source of the item in dispute or from public records confirming that the report was inaccurate or incomplete, unless the consumer reporting agency, in the exercise of good faith and reasonable judgment, has substantial reason based on specific, verifiable facts to doubt the authenticity of the documentation submitted and notifies the consumer in writing of that decision, explaining its reasons for unblocking the information and setting forth the specific, verifiable facts on which the decision was based.

(m) Any provision in a contract that prohibits the disclosure of a credit score by a

person who makes or arranges loans or a consumer credit reporting agency is void. A lender shall not have liability under any contractual provision for disclosure of a credit score.

1785.16.1. A consumer credit reporting agency shall delete from a consumer credit report inquiries for credit reports based upon credit requests that the consumer credit reporting agency verifies were initiated as the result of identity theft, as defined in Section 1798.92.

1785.16.2. (a) No creditor may sell a consumer debt to a debt collector, as defined in 15 U.S.C. Sec. 1692a, if the consumer is a victim of identity theft, as defined in Section 1798.2, and with respect to that debt, the creditor has received notice pursuant to subdivision (k) of Section 1785.16.

(b) Subdivision (a) does not apply to a creditor's sale of a debt to a subsidiary or affiliate of the creditor, if, with respect to that debt, the subsidiary or affiliate does not take any action to collect the debt.

(c) For the purposes of this section, the requirement in 15 U.S.C. Sec. 1692a, that a person must use an instrumentality of interstate commerce or the mails in the collection of any debt to be considered a debt collector, does not apply.

1785.19. (a) In addition to any other remedy provided by law, a consumer may bring an action for a civil penalty, not to exceed two thousand five hundred dollars ($2,500), against any of the following:

(1) A person who knowingly and willfully obtains access to a file other than as provided in Section 1785.11.

(2) Any person who knowingly and willfully obtains data from a file other than as provided in Section 1785.11.

(3) A person who uses the data received from a file in a manner contrary to an agreement with the consumer credit reporting agency.

Such an action may also be brought by the person or entity responsible for the file accessed. This remedy is in addition to any other remedy which may exist.

(b) If a plaintiff prevails in an action under subdivision (a) he or she shall be awarded the civil penalty, costs, and reasonable attorney fees.

1785.20.3. (a) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, and who discovers that the consumer's first and last name, address, or social security number, on the credit application does not match, within a reasonable degree of certainty, the consumer's first and last name, address or addresses, or social security number listed, if any, on the consumer credit report, shall take reasonable steps to verify the accuracy of the consumer's first and last name, address, or social security number provided on the application to confirm that the extension of credit is not the result of identity theft, as defined in Section 1798.92.

(b) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, and who has received notification pursuant to subdivision (k) of Section 1785.16 that the applicant has been a victim of identity theft, as defined in Section 1798.92, may not lend money or extend credit without taking reasonable steps to verify the consumer' s identity and confirm that

the application for an extension of credit is not the result of identity theft.

(c) Any consumer who suffers damages as a result of a violation of this section by any person may bring an action in a court of appropriate jurisdiction against that person to recover actual damages, court costs, attorney's fees, and punitive damages of not more than thirty thousand dollars ($30,000) for each violation, as the court deems proper.

(d) As used in this section, "identity theft" has the meaning given in subdivision (b) of Section 1798.92.

(e) For the purposes of this section, "extension of credit" does not include an increase in an existing open-end credit plan, as defined in Regulation Z of the Federal Reserve System (12 C.F.R. 226.2), or any change to or review of an existing credit account.

(f) If a consumer provides initial written notice to a creditor that he or she is a victim of identity theft, as defined in subdivision (d) of Section 1798.92, the creditor shall provide written notice to the consumer of his or her rights under subdivision (k) of Section 1785.16.

(g) The provisions of subdivisions (k) and (l) of Section 1785.16 do not apply to a consumer credit reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer credit reporting agency or the databases of multiple consumer credit reporting agencies, and does not maintain a permanent database of credit information from which new credit reports are produced.

(h) This section does not apply if one of the addresses at issue is a United States Army or Air Force post office address or a United States Fleet post office address.

1788.10. No debt collector shall collect or attempt to collect a consumer debt by means of the following conduct:

(a) The use, or threat of use, of physical force or violence or any criminal means to cause harm to the person, or the reputation, or the property of any person;

(b) The threat that the failure to pay a consumer debt will result in an accusation that the debtor has committed a crime where such accusation, if made, would be false;

(c) The communication of, or threat to communicate to any person the fact that a debtor has engaged in conduct, other than the failure to pay a consumer debt, which the debt collector knows or has reason to believe will defame the debtor;

(d) The threat to the debtor to sell or assign to another person the obligation of the debtor to pay a consumer debt, with an accompanying false representation that the result of such sale or
assignment would be that the debtor would lose any defense to the consumer debt;

(e) The threat to any person that nonpayment of the consumer debt may result in the arrest of the debtor or the seizure, garnishment, attachment or sale of any property or the garnishment or attachment of wages of the debtor, unless such action is in fact contemplated by the debt collector and permitted by the law; or

(f) The threat to take any action against the debtor which is prohibited by this title.

1788.11. No debt collector shall collect or attempt to collect a consumer debt by means of the following practices:

(a) Using obscene or profane language;

(b) Placing telephone calls without disclosure of the caller's identity, provided that an employee of a licensed collection agency may identify himself by using his registered

alias name as long as he correctly identifies the agency he represents;

(c) Causing expense to any person for long distance telephone calls, telegram fees or charges for other similar communications, by misrepresenting to such person the purpose of such telephone call, telegram or similar communication;

(d) Causing a telephone to ring repeatedly or continuously to annoy the person called; or

(e) Communicating, by telephone or in person, with the debtor with such frequency as to be unreasonable and to constitute an harassment to the debtor under the circumstances.

1788.12. No debt collector shall collect or attempt to collect a consumer debt by means of the following practices:

(a) Communicating with the debtor's employer regarding the debtor's consumer debt unless such a communication is necessary to the collection of the debt, or unless the debtor or his attorney has consented in writing to such communication. A communication is necessary to the collection of the debt only if it is made for the purposes of verifying the debtor's employment, locating the debtor, or effecting garnishment, after judgment, of the debtor's wages, or in the case of a medical debt for the purpose of discovering the existence of medical insurance. Any such communication, other than a communication in the case of a medical debt by a health care provider or its agent for the purpose of discovering the existence of medical insurance, shall be in writing unless such written communication receives no response within 15 days and shall be made only as many times as is necessary to the collection of the debt. Communications to a debtor's employer regarding a debt shall not contain language that would be improper if the communication were made to the debtor. One communication solely for the purpose of verifying the debtor's employment may be oral without prior written contact.

(b) Communicating information regarding a consumer debt to any member of the debtor's family, other than the debtor's spouse or the parents or guardians of the debtor who is either a minor or who resides in the same household with such parent or guardian, prior to obtaining a judgment against the debtor, except where the purpose of the communication is to locate the debtor, or where the debtor or his attorney has consented in writing to such communication;

(c) Communicating to any person any list of debtors which discloses the nature or existence of a consumer debt, commonly known as "deadbeat lists", or advertising any consumer debt for sale, by naming the debtor; or

(d) Communicating with the debtor by means of a written communication that displays or conveys any information about the consumer debt or the debtor other than the name, address and telephone number of the debtor and the debt collector and which is intended both to be seen by any other person and also to embarrass the debtor.

(e) Notwithstanding the foregoing provisions of this section, the disclosure, publication or communication by a debt collector of information relating to a consumer debt or the debtor to a consumer reporting agency or to any other person reasonably believed to have a legitimate business need for such information shall not be deemed to violate this title.

1788.13. No debt collector shall collect or attempt to collect a consumer debt by means of the following practices:

(a) Any communication with the debtor other than in the name either of the debt

collector or the person on whose behalf the debt collector is acting;

(b) Any false representation that any person is an attorney or counselor at law;

(c) Any communication with a debtor in the name of an attorney or counselor at law or upon stationery or like written instruments bearing the name of the attorney or counselor at law, unless such communication is by an attorney or counselor at law or shall have been approved or authorized by such attorney or counselor at law;

(d) The representation that any debt collector is vouched for, bonded by, affiliated with, or is an instrumentality, agent or official of any federal, state or local government or any agency of federal, state or local government, unless the collector is actually employed by the particular governmental agency in question and is acting on behalf of such agency in the debt collection matter;

(e) The false representation that the consumer debt may be increased by the addition of attorney's fees, investigation fees, service fees, finance charges, or other charges if, in fact, such
fees or charges may not legally be added to the existing obligation;

(f) The false representation that information concerning a debtor' s failure or alleged failure to pay a consumer debt has been or is about to be referred to a consumer reporting agency;

(g) The false representation that a debt collector is a consumer reporting agency;

(h) The false representation that collection letters, notices or other printed forms are being sent by or on behalf of a claim, credit, audit or legal department;

(i) The false representation of the true nature of the business or services being rendered by the debt collector;

(j) The false representation that a legal proceeding has been, is about to be, or will be instituted unless payment of a consumer debt is made;

(k) The false representation that a consumer debt has been, is
about to be, or will be sold, assigned, or referred to a debt
collector for collection; or

(l) Any communication by a licensed collection agency to a debtor demanding money unless the claim is actually assigned to the collection agency.

1788.14. No debt collector shall collect or attempt to collect a consumer debt by means of the following practices:

(a) Obtaining an affirmation from a debtor who has been adjudicated a bankrupt, of a consumer debt which has been discharged in such bankruptcy, without clearly and conspicuously disclosing to the debtor, in writing, at the time such affirmation is sought, the fact that the debtor is not legally obligated to make such affirmation;

(b) Collecting or attempting to collect from the debtor the whole or any part of the debt collector's fee or charge for services rendered, or other expense incurred by the debt collector in the collection of the consumer debt, except as permitted by law; or

(c) Initiating communications, other than statements of account, with the debtor with regard to the consumer debt, when the debt collector has been previously notified in writing by the debtor's
attorney that the debtor is represented by such attorney with respect to the consumer debt and such notice includes the attorney's name and address and a request by such attorney that all communications regarding the consumer debt be addressed to such attorney,

unless the attorney fails to answer correspondence, return telephone calls, or discuss the obligation in question. This subdivision shall not apply where prior approval has been obtained from the debtor's attorney, or where the communication is a response in the ordinary course of business to a debtor's inquiry.

1788.15. (a) No debt collector shall collect or attempt to collect a consumer debt by means of judicial proceedings when the debt collector knows that service of process, where essential to jurisdiction over the debtor or his property, has not been legally effected.

(b) No debt collector shall collect or attempt to collect a consumer debt, other than one reduced to judgment, by means of judicial proceedings in a county other than the county in which the debtor has incurred the consumer debt or the county in which the debtor resides at the time such proceedings are instituted, or resided at the time the debt was incurred.

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

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

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

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

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

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

(f) For purposes of this section, "personal information" does not include publicly

available information that is lawfully made available to the general public from federal, state, or local government records.

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

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be
notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

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

(C) Notification to major statewide media.

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

1798.81. A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

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

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency

determines that it will not compromise the investigation.

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

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

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

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

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

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

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

1798.83. (a) Except as otherwise provided in subdivision (d), if a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information that corresponds to any of the categories of personal information set forth in paragraph (6) of subdivision (e) to third

parties, and if the business knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer, provide all of the following information to the customer free of charge:

(1) In writing or by electronic mail, a list of the categories set forth in paragraph (6) of subdivision (e) that correspond to the personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year.

(2) In writing or by electronic mail, the names and addresses of all of the third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding calendar year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.

(b) (1) A business required to comply with this section shall designate a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone or facsimile, a toll-free telephone or facsimile number, to which customers may deliver requests pursuant to subdivision (a). A business required to comply with this section shall, at its election, do at least one of the following:

(A) Notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or numbers or the means to obtain those addresses or numbers and instruct those employees that customers who inquire about the business's privacy practices or the business's compliance with this section shall be informed of the designated addresses or numbers or the means to obtain the addresses or numbers.

(B) Add to the home page of its Web site a link either to a page titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the home page's link to the business's privacy policy. If the business elects to add the words "Your Privacy Rights" to the link to the business's privacy policy, the words "Your Privacy Rights" shall be in the same style and size as the link to the business's privacy policy. If the business does not display a link to its privacy policy on the home page of its Web site, or does not have a privacy policy, the words "Your Privacy Rights" shall be written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language. The first page of the link shall describe a customer's rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words "Your California Privacy Rights" to the home page's link to the business's privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer's rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers.

(C) Make the designated addresses or numbers, or means to obtain the designated addresses or numbers, readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers.

The response to a request pursuant to this section received at one of the designated addresses or numbers shall be provided within 30 days. Requests received by the business at other than one of the designated addresses or numbers shall be provided within a reasonable period, in light of the circumstances related to how the request was received, but not to exceed 150 days from the date received.

(2) A business that is required to comply with this section and Section 6803 of Title 15 of the United States Code may comply with this section by providing the customer the disclosure required by Section 6803 of Title 15 of the United States Code, but only if the disclosure also complies with this section.

(3) A business that is required to comply with this section is not obligated to provide information associated with specific individuals and may provide the information required by this section in standardized format.

1798.85. (a) Except as provided in this section, a person or entity may not do any of the following:

(1) Publicly post or publicly display in any manner an individual's social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding this paragraph, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security number. A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(b) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative purposes.

(c) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), Chapter 14 (commencing with Section 7150) or Chapter 14.5 (commencing with Section 7220) of Division 7 of Title 1 of, Article 9 (commencing with Section 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter 9 (commencing with Section 54950) of Part 1 of

Division 2 of Title 5 of, the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made available to the public by entities provided for in Article VI of the California Constitution.

(d) (1) In the case of a health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor as defined in Section 56.05, or the provision by any person or entity of administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only, this section shall become operative in the following manner:

(A) On or before January 1, 2003, the entities listed in paragraph (1) shall comply with paragraphs (1), (3), (4), and (5) of subdivision (a) as these requirements pertain to individual policyholders or individual contract holders.

(B) On or before January 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) as these requirements pertain to new individual policyholders or new individual contract holders and new groups, including new groups administered or issued on or after January 1, 2004.

(C) On or before July 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) for all individual policyholders and individual contract holders, for all groups, and for all enrollees of the Healthy Families and Medi-Cal programs, except that for individual policyholders, individual contract holders and groups in existence prior to January 1, 2004, the entities listed in paragraph (1) shall comply upon the renewal date of the policy, contract, or group on or after July 1, 2004, but no later than July 1, 2005.

(2) A health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor, or another person or entity as described in paragraph (1) shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this article are implemented on or before the dates specified in this section.

(3) Notwithstanding paragraph (2), the Director of the Department of Managed Health Care, pursuant to the authority granted under Section 1346 of the Health and Safety Code, or the Insurance Commissioner, pursuant to the authority granted under Section 12921 of the Insurance Code, and upon a determination of good cause, may grant extensions not to exceed six months for compliance by health care service plans and insurers with the requirements of this section when requested by the health care service plan or insurer. Any extension granted shall apply to the health care service plan or insurer's affected providers, pharmacy benefits manager, and contractors.

(e) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, a provider of health care, a health care service plan, a licensed health care professional, or a contractor, as those terms are defined in Section 56.05, that complies with the federal law shall be deemed in compliance with this section.

(f) A person or entity may not encode or embed a social security number in or on a card or document, including, but not limited to, using a barcode, chip, magnetic strip, or other technology, in place of removing the social security number, as required by this section.

(g) This section shall become operative, with respect to the University of California, in

the following manner:

(1) On or before January 1, 2004, the University of California shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the University of California shall comply with paragraphs (4) and (5) of subdivision (a).

(h) This section shall become operative with respect to the Franchise Tax Board on January 1, 2007.

(i) This section shall become operative with respect to the California community college districts on January 1, 2007.

(j) This section shall become operative with respect to the California State University system on July 1, 2005.

(k) This section shall become operative, with respect to the California Student Aid Commission and its auxiliary organization, in the following manner:

(1) On or before January 1, 2004, the commission and its auxiliary organization shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the commission and its auxiliary organization shall comply with paragraphs (4) and (5) of subdivision (a).

1798.90.1. (a) (1) Any business may swipe a driver's license or identification card issued by the Department of Motor Vehicles in any electronic device for the following purposes:

(A) To verify age or the authenticity of the driver's license or identification card.

(B) To comply with a legal requirement to record, retain, or transmit that information.

(C) To transmit information to a check service company for the purpose of approving negotiable instruments, electronic funds transfers, or similar methods of payments, provided that only the name and identification number from the license or the card may be used or retained by the check service company.

(D) To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation.

(2) A business may not retain or use any of the information obtained by that electronic means for any purpose other than as provided herein.

(b) As used in this section, "business" means a proprietorship, partnership, corporation, or any other form of commercial enterprise.

(c) A violation of this section constitutes a misdemeanor punishable by imprisonment in a county jail for no more than one year, or by a fine of no more than ten thousand dollars ($10,000), or by both.

1798.93. (a) A person may bring an action against a claimant to establish that the person is a victim of identity theft in connection with the claimant's claim against that person. If the claimant has brought an action to recover on its claim against the person, the person may file a cross-complaint to establish that the person is a victim of identity theft in connection with the claimant's claim.

(b) A person shall establish that he or she is a victim of identity theft by a preponderance of the evidence.

(c) A person who proves that he or she is a victim of identity theft, as defined in Section 530.5 of the Penal Code, as to a particular claim, shall be entitled to a judgment providing all of the following, as appropriate:

(1) A declaration that he or she is not obligated to the claimant on that claim.

(2) A declaration that any security interest or other interest the claimant had purportedly obtained in the victim's property in connection with that claim is void and unenforceable.

(3) An injunction restraining the claimant from collecting or attempting to collect from the victim on that claim, from enforcing or attempting to enforce any security interest or other interest in the victim's property in connection with that claim, or from enforcing or executing on any judgment against the victim on that claim.

(4) If the victim has filed a cross-complaint against the claimant, the dismissal of any cause of action in the complaint filed by the claimant based on a claim which arose as a result of the identity theft.

(5) Actual damages, attorney's fees, and costs, and any equitable relief that the court deems appropriate. In order to recover actual damages or attorney's fees in an action or cross-complaint filed by a person alleging that he or she is a victim of identity theft, the person shall show that he or she provided written notice to the claimant that a situation of identity theft might exist, including, upon written request of the claimant, a valid copy of the police report or the Department of Motor Vehicles investigative report promptly filed pursuant to Section 530.5 of the Penal Code at least 30 days prior to his or her filing of the action, or within his or her cross-complaint pursuant to this section.

(6) A civil penalty, in addition to any other damages, of up to thirty thousand dollars ($30,000) if the victim establishes by clear and convincing evidence all of the following:

(A) That at least 30 days prior to filing an action or within the cross-complaint pursuant to this section, he or she provided written notice to the claimant at the address designated by the claimant for complaints related to credit reporting issues that a situation of identity theft might exist and explaining the basis for that belief.

(B) That the claimant failed to diligently investigate the victim's notification of a possible identity theft.

(C) That the claimant continued to pursue its claim against the victim after the claimant was presented with facts that were later held to entitle the victim to a judgment pursuant to this section.

2.2.3. *Financial Code*

22342. (a) As used in this section, "instant loan check" or "live check" means any loan or extension of credit that is made available in the form of a check, draft, or any other negotiable instrument that can be deposited in a bank or used for third-party payments. "Instant loan check" or "live check" does not include a check, draft, or any other negotiable instrument provided in response to an application for credit or as a means of access to an existing loan or extension of credit, including a home equity or personal line of credit.

(b) No person shall produce, advertise, offer, sell, distribute, or otherwise transfer for use in this state any live check unless the document bears the following phrase printed in 12-point type on the front of the document: "THIS IS A LOAN OR AN EXTENSION OF CREDIT. YOU WILL PAY CHARGES."

(c) Live checks shall only be negotiable for a period of 30 days after the date printed on

the live check. Printed material accompanying the live check shall advise the consumer to void and destroy the live check if it is not going to be negotiated.

(d) Loan solicitations shall be mailed in envelopes with no indication that a negotiable instrument is contained in the mailing. Envelopes shall be marked with "do not forward" instructions to the postal service in the event that the intended addressee is no longer at the location.

(e) Any loan solicitation made through a live check shall be honored in the full amount by the issuer unless the account on which the solicitation is made is closed by the consumer prior to the date the check is cashed.

(f) In the event that a live check is stolen or incorrectly received by someone other than the intended payee, and the live check is cashed or otherwise negotiated based upon fraud or misrepresentation by someone other than the intended payee, the following safeguards for the consumer shall apply:

(1) The creditor, upon receipt of notification that the consumer did not negotiate the live check and is a victim of identity theft as defined in Section 1798.92 of the Civil Code, shall provide, and the consumer may complete, a statement confirming that the consumer did not deposit, cash, or otherwise negotiate the live check.

(2) Upon completion of the confirmation statement by the consumer, the consumer who was the intended payee shall have no liability for the loan obligation, absent any fraud by that consumer.

(3) Upon receipt of notification that the consumer did not negotiate the live check and is a victim of identity theft as defined in Section 1798.92 of the Civil Code, the creditor shall take appropriate actions set forth in Sections 1785.25 and 1785.26 of the Civil Code.

(g) The commissioner may, after appropriate notice and opportunity for hearing, by order levy administrative penalties against a licensee who violates this section, and the licensee shall be liable for administrative penalties of no more than two thousand five hundred dollars ($2,500) for each willful violation. Any hearing shall be held in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500) of Part 1 of Division 3 of Title 2 of the Government Code), and the commissioner shall have all the powers granted under the act. The remedy available under this subdivision is in addition to any other remedies available to the commissioner under this division that may be employed to enforce the provisions of this section.

(h) Nothing in this section shall preclude the application of any section or rule under this division.

4052.5. Except as provided in Sections 4053, 4054.6, and 4056, a financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information to or with any nonaffiliated third parties without the explicit prior consent of the consumer to whom the nonpublic personal information relates.

2.2.4. *Family Code*

2024.5. (a) Except as provided in subdivision (b), the petitioner or respondent may redact any social security number from any pleading, attachment, document, or other written material filed with the court pursuant to a petition for dissolution of marriage,

nullity of marriage, or legal separation. The Judicial Council form used to file such a petition, or a response to such a petition, shall contain a notice that the parties may redact any social security numbers from those pleadings, attachments, documents, or other material filed with the court.

(b) An abstract of support judgment, the form required pursuant to subdivision (b) of Section 4014, or any similar form created for the purpose of collecting child or spousal support payments may not be redacted pursuant to subdivision (a).

2.2.5. *Health and Safety Code*

103526. (a) If the State Registrar, local registrar, or county recorder receives a written or faxed request for a certified copy of a birth or death record pursuant to Section 103525, or a military service record pursuant to Section 6107 of the Government Code, that is accompanied by a notarized statement sworn under penalty of perjury, or a faxed copy of a notarized statement sworn under penalty of perjury, that the requester is an authorized person, as defined in this section, that official may furnish a certified copy to the applicant in accordance with Section 103525 and in accordance with Section 6107 of the Government Code. If a written request for a certified copy of a military service record is submitted to a county recorder by fax, the county recorder may furnish a certified copy of the military record to the applicant in accordance with Section 103525. A faxed notary acknowledgment accompanying a faxed request received pursuant to this subdivision for a certified copy of a birth or death record or a military service record shall be legible and, if the notary's seal is not photographically reproducible, show the name of the notary, the county of the notary's principal place of business, the notary's telephone number, the notary's registration number, and the notary's commission expiration date typed or printed in a manner that is photographically reproducible below, or immediately adjacent to, the notary's signature in the acknowledgment. If a request for a certified copy of a birth or death record is made in person, the official shall take a statement sworn under penalty of perjury that the requester is signing his or her own legal name and is an authorized person, and that official may then furnish a certified copy to the applicant.

(b) In all other circumstances, the certified copy provided to the applicant shall be an informational certified copy and shall display a legend that states "INFORMATIONAL, NOT A VALID DOCUMENT TO ESTABLISH IDENTITY." The legend shall be placed on the certificate in
a manner that will not conceal information.

(c) For purposes of this section, an "authorized person" is any of the following:

(1) The registrant or a parent or legal guardian of the registrant.

(2) A party entitled to receive the record as a result of a court order, or an attorney or a licensed adoption agency seeking the birth record in order to comply with the requirements of Section 3140 or 7603 of the Family Code.

(3) A member of a law enforcement agency or a representative of another governmental agency, as provided by law, who is conducting official business.

(4) A child, grandparent, grandchild, sibling, spouse, or domestic partner of the registrant.

(5) An attorney representing the registrant or the registrant's estate, or any person or

agency empowered by statute or appointed by a court to act on behalf of the registrant or the registrant's estate.

(6) Any agent or employee of a funeral establishment who acts within the course and scope of his or her employment and who orders certified copies of a death certificate on behalf of any individual specified in paragraphs (1) to (5), inclusive, of subdivision (a) of Section 7100.

(d) Any person who asks the agent or employee of a funeral establishment to request a death certificate on his or her behalf warrants the truthfulness of his or her relationship to the decedent,
and is personally liable for all damages occasioned by, or resulting from, a breach of that warranty.

(e) Notwithstanding any other provision of law:

(1) Any member of a law enforcement agency or a representative of a state or local government agency, as provided by law, who orders a copy of a record to which subdivision (a) applies in conducting official business may not be required to provide the notarized statement required by subdivision (a).

(2) An agent or employee of a funeral establishment who acts within the course and scope of his or her employment and who orders death certificates on behalf of individuals specified in paragraphs (1) to (5), inclusive, of subdivision (a) of Section 7100 shall not be required to provide the notarized statement required by subdivision (a).

(f) Informational certified copies of birth and death certificates issued pursuant to subdivision (b) shall only be printed from the single statewide database prepared by the State Registrar and shall be electronically redacted to remove any signatures for purposes of compliance with this section. Local registrars and county recorders shall not issue informational certified copies of birth and death certificates from any source other than the statewide database prepared by the State Registrar. This subdivision shall become operative on July 1, 2007, but only after the statewide database becomes operational and the full calendar year of the birth and death indices and images is entered into the statewide database and is available for the respective year of the birth or death certificate for which an informational copy is requested. The State Registrar shall provide written notification to local registrars and county recorders as soon as a year becomes available for issuance from the statewide database.

2.2.6. *Business and Professions Code*

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

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

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

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

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

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

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

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

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

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

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

2.2.7. *Elections Code*

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.(b) For purposes of this section, "United States" includes each of the several states of the United States, the District of Columbia, and the territories and possessions of the United States.