Order Code RL31919

CRS Report for Congress

Remedies Available to Victims of Identity Theft

Updated April 19, 2005

Angie A. Welborn
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Remedies Available to Victims of Identity Theft

Summary

According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all fifty states, and complaints regarding identity theft have grown for four consecutive years. Victims of identity theft may incur damaged credit records, unauthorized charges on credit cards, and unauthorized withdrawals from bank accounts. Sometimes, victims must change their telephone numbers or even their social security numbers. Victims may also need to change addresses that were falsified by the impostor.

This report provides an overview of the federal laws that could assist victims of identity theft with purging inaccurate information from their credit records and removing unauthorized charges from credit accounts, as well as federal laws that impose criminal penalties on those who assume another person's identity through the use of fraudulent identification documents. Relevant state laws and pending federal legislation are also discussed (H.R. 1263, H.R. 1099, H.R. 1080, H.R. 1078, H.R. 220, S. 768, S. 751, S. 500, S. 472, S. 116, S. 115 and S. 29). This report will be updated as events warrant.

Contents

Remedies Available to Victims of Identity Theft

Federal Laws Related to Identity Theft

Identity Theft Assumption and Deterrence Act. While not exclusively aimed at consumer identity theft, the Identity Theft Assumption Deterrence Act prohibits fraud in connection with identification documents under a variety of circumstances.[1] Certain offenses under the statute relate directly to consumer identity theft, and impostors could be prosecuted under the statute. For example, the statute makes it a federal crime, under certain circumstances,[2] to knowingly and without lawful authority produce an identification document[3] or false identification document; or to knowingly possess an identification document that is or appears to be an identification document of the United States which is stolen or produced without lawful authority knowing that such document was stolen or produced without such authority.[4] It is also a federal crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or

---

[1] 18 U.S.C. 1028. The statute lists several actions that constitute fraud in connection with identification documents. However, for the purposes of this report, they do not all relate to consumer-related identity theft, i.e. situations where a consumer's Social Security number or driver's license number may be stolen and used to establish credit accounts by an impostor.

[2] According to the statute, the prohibitions listed apply when "the identification document 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 or false identification document;" the document is presented with the intent to defraud the United States; or "either 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 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." 18 U.S.C. 1028(c).

[3] Identification document is defined as "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 internal 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." 18 U.S.C. 1028(d)(2). Identification documents include Social Security cards, birth certificates, driver's licenses, and personal identification cards.

[4] 18 U.S.C. 1028(a)(1) and (2).

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.[5]

The punishment for offenses involving fraud related to identification documents varies depending on the specific offense and the type of document involved.[6] For example, a fine or imprisonment of up to 15 years may be imposed for using the identification of another person with the intent to commit any unlawful activity under state law, if, as a result of the offense, the person committing the offense obtains anything of value totaling $1,000 or more during any one-year period.[7] Other offenses carry terms of imprisonment up to three years.[8] However, if the offense is committed to facilitate a drug trafficking crime or in connection with a crime of violence, the term of imprisonment could be up to twenty years.[9] Offenses committed to facilitate an action of international terrorism are punishable by terms of imprisonment up to twenty-five years.[10]

Identity Theft Penalty Enhancement Act. The Identity Theft Penalty Enhancement Act was signed by the President on July 15, 2004, (P.L. 108-275). The act amends Title 18 of the United States Code to define and establish penalties for aggravated identity theft and makes changes to the existing identity theft provisions of Title 18. Under the new law, aggravated identity theft occurs when a person "knowingly transfers, possess, or uses, without lawful authority, a means of identification of another person" during and in relation to the commission of certain enumerated felonies.[11] The penalty for aggravated identity theft is a term of imprisonment of two years in addition to the punishment provided for the original felony committed. Offenses committed in conjunction with certain terrorism offenses are subject to an additional term of imprisonment of five years. The act also directs the United States Sentencing Commission to "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" adhering to certain requirements outlined in the legislation.[12]

---

[5] 18 U.S.C. 1028(a)(7).

[6] 18 U.S.C. 1028(b).

[7] 18 U.S.C. 1028(b)(1)(D).

[8] 18 U.S.C. 1028(b)(2).

[9] 18 U.S.C. 1028(b)(3).

[10] 18 U.S.C. 1028(b)(4).

[11] P.L. 108-275, Sec. 2, to be codified at 18 U.S.C. 1028A. Offenses that could give rise to aggravated identity theft are enumerated in this section, and include offenses relating to theft of public money, property, or rewards; theft, embezzlement, or misapplication by a bank officer or employee; theft from employee benefit plans; false personation of citizenship; false statements in connection with the acquisition of a firearm; mail, bank, and wire fraud; obtaining consumer information by false pretenses; and certain immigration violations. The list of enumerated offenses will be codified at 18 U.S.C. 1028A(c).

[12] P.L. 108-275, Sec. 5.

In addition to increasing penalties for identity theft, the act authorized appropriations to the Justice Department "for the investigation and prosecution of identity theft and related credit card and other fraud cases constituting felony violations of law, $2,000,000 for FY2005 and $2,000,000 for each of the 4 succeeding fiscal years."[13]

Fair Credit Reporting Act. While the Fair Credit Reporting Act (FCRA) does not directly address identity theft, it could offer victims assistance in having negative information resulting from unauthorized charges or accounts removed from their credit files.[14] The purpose of the FCRA 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."[15] The FCRA outlines a consumer's rights in relation to his or her credit report, as well as permissible uses for credit reports and disclosure requirements. In addition, the FCRA imposes a duty on consumer reporting agencies to ensure that the information they report is accurate, and requires persons who furnish information to ensure that the information they furnish is accurate.

The FCRA allows consumers to file suit for violations of the act, which could include the disclosure of inaccurate information about a consumer by a credit reporting agency.[16] A consumer who is a victim of identity theft could file suit against a credit reporting agency for the agency's failure to verify the accuracy of information contained in the report and the agency's disclosure of inaccurate information as a result of the consumer's stolen identity. Under the FCRA, as recently amended, a consumer may file suit not later than the earlier of two years after the date of discovery by the plaintiff of the violation that is the basis for such liability, or five years after the date on which the violation occurred.[17]

Fair and Accurate Credit Transactions (FACT) Act of 2003. The FACT Act, signed by the President on December 4, 2003, includes, *inter alia*, a number of amendments to the Fair Credit Reporting Act aimed at preventing identity theft and assisting victims.[18] Generally, these new provisions mirror laws passed by

---

[13] P.L. 108-275, Sec. 6.

[14] For more information on a consumer's rights under the FCRA, see CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities.*

[15] 15 U.S.C. 1681(b).

[16] 15 U.S.C. 1681n; 15 U.S.C. 1681o. For more information see CRS Report RS21083, *Identity Theft and the Fair Credit Reporting Act: An Analysis of* TRW v. Andrews *and Current Legislation.*

[17] P.L. 108-159, Section 156.

[18] P.L. 108-159. For effective dates, see 68 FR 74467 and 68 FR 74529 (December 24, 2003).

state legislatures and create a national standard for addressing consumer concerns with regard to identity theft and other types of fraud.[19]

Credit card issuers, who operate as users of consumer credit reports, are required, under a new provision of the FCRA, to follow certain procedures when the issuer receives a request for an additional or replacement card within a short period of time following notification of a change of address for the same account.[20] In a further effort to prevent identity theft, other new provisions require the truncation of credit card account numbers on electronically printed receipts,[21] and, upon request, the truncation of social security numbers on credit reports provided to a consumer.[22]

Consumers who have been victims of identity theft, or expect that they may become victims, are now able to have fraud alerts placed in their files.[23] Pursuant to the new provisions, a consumer may request a fraud alert from one consumer reporting agency and that agency is required to notify the other nationwide consumer reporting agencies of the existence of the alert. In general, fraud alerts are to be maintained in the file for 90 days, but a consumer may request an extended alert which is maintained for up to seven years. The fraud alert becomes a part of the consumer's credit file and is thus passed along to all users of the report. The alert must also be included with any credit score generated using the consumer's file, and must be referred to other consumer reporting agencies.[24]

In addition to the fraud alert, victims of identity theft may also have information resulting from the crime blocked from their credit reports.[25] After the receipt of appropriate proof of the identity of the consumer, a copy of an identity theft report, the identification of the alleged fraudulent information, and a statement by the consumer that the information is not information relating to any transaction conducted by the consumer, a consumer reporting agency must block all such information from being reported and must notify the furnisher of the information in question that it may be the result of identity theft. Requests for the blocking of information must also be referred to other consumer reporting agencies.[26]

Victims of identity theft are also allowed to request information about the alleged crime. A business entity is required, upon request and subject to verification of the victim's identity, to provide copies of application and business transaction records evidencing any transaction alleged to be a result of identity theft to the victim

---

[19] Generally, many of these new federal provisions preempt similar state laws. For more information on the preemptive effects of the Fair Credit Reporting Act, see CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law.*

[20] P.L. 108-159, Section 114.

[21] P.L. 108-159, Section 113.

[22] P.L. 108-159, Section 115.

[23] P.L. 108-159, Section 112.

[24] P.L. 108-159, Section 153.

[25] P.L. 108-159, Section 152.

[26] P.L. 108-159, Section 153.

or to any law enforcement agency investigating the theft and authorized by the victim to take receipt of the records in question.[27]

Fair Credit Billing Act. The Fair Credit Billing Act (FCBA) is not an identity theft statute *per se*, but it does provide consumers with an opportunity to receive an explanation and proof of charges that may have been made by an impostor and to have unauthorized charges removed from their accounts. The purpose of the FCBA is "to protect the consumer against inaccurate and unfair credit billing and credit card practices."[28] The law defines and establishes a procedure for resolving billing errors in consumer credit transactions. For purposes of the FCBA, a "billing error" includes unauthorized charges, charges for goods or services not accepted by the consumer or delivered to the consumer, and charges for which the consumer has asked for an explanation or written proof of purchase.[29]

Under the FCBA, consumers are able to file a claim with the creditor to have billing errors resolved. Until the alleged billing error is resolved, the consumer is not required to pay the disputed amount, and the creditor may not attempt to collect, any part of the disputed amount, including related finance charges or other charges.[30] The act sets forth dispute resolution procedures and requires an investigation into the consumer's claims. If the creditor determines that the alleged billing error did occur, the creditor is obligated to correct the billing error and credit the consumer's account with the disputed amount and any applicable finance charges.[31]

Electronic Fund Transfer Act. Similar to the Fair Credit Billing Act, the Electronic Fund Transfer Act is not an identity theft statute *per se*, but it does provide consumers with a mechanism for challenging unauthorized transactions and having their accounts recredited in the event of an error. The purpose of the Electronic Fund Transfer Act (EFTA) is to "provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems."[32] Among other things, the EFTA limits a consumer's liability for unauthorized electronic fund transfers. If the consumer notifies the financial institution within two business days after learning of the loss or theft of a debt card or other device used to make electronic transfers, the consumer's liability is limited to the lesser of $50 or the amount of the unauthorized transfers that occurred before notice was given to the financial institution.[33]

Additionally, financial institutions are required to provide a consumer with documentation of all electronic fund transfers initiated by the consumer from an electronic terminal. If a financial institution receives, within 60 days after providing

---

[27] P.L. 108-159, Section 151.

[28] 15 U.S.C. 1601(a).

[29] 15 U.S.C. 1666(b); 12 C.F.R. 226.13(a).

[30] 15 U.S.C. 1666(c); 12 C.F.R. 226.13(d)(1).

[31] 15 U.S.C. 1666(a); 12 C.F.R. 226.13(e).

[32] 15 U.S.C. 1693(b).

[33] 15 U.S.C. 1693g(a), 12 C.F.R. 205.6(b)(1).

such documentation, an oral or written notice from the consumer indicating the consumer's belief that the documentation provided contains an error, the financial institution must investigate the alleged error, determine whether an error has occurred, and report or mail the results of the investigation and determination to the consumer within ten business days.[34] The notice from the consumer to the financial institution must identify the name and account number of the consumer; indicate the consumer's belief that the documentation contains an error and the amount of the error; and set forth the reasons for the consumer's belief that an error has occurred.[35]

In the event that the financial institution determines that an error has occurred, the financial institution must correct the error within one day of the determination in accordance with the provisions relating to the consumer's liability for unauthorized charges.[36] The financial institution may provisionally recredit the consumer's account for the amount alleged to be in error pending the conclusion of its investigation and its determination of whether an error has occurred, if it is unable to complete the investigation within ten business days.[37]

State Identity Theft Statutes

State Criminal Laws. Most states have enacted some type of criminal identity theft statute.[38] Many of these statutes impose criminal monetary penalties for identity theft activities. For example, in California, impostors are subject to fines of up to $10,000 and confinement in jail for up to one year.[39] Restitution may also be a component of the impostor's punishment. In Texas, identity theft is a felony and, in addition to jail time, the court may order the impostor to reimburse the victim for lost income and other expenses incurred as a result of the theft.[40] Other states impose civil penalties and provide victims with judicial recourse for damages incurred as a result of the theft. In Washington, impostors are "liable for civil damages of five hundred dollars or actual damages, whichever is greater, including costs to repair the victim's credit record."[41]

While some statutes may define identity theft to include only the fraudulent use of identification documents, other statutes may more broadly define such activities. For example, Oregon also criminalizes the fraudulent use of credit cards. Such use constitutes a felony if the "aggregate total amount of property or services the person

---

[34] 15 U.S.C. 1693f(a), 12 C.F.R. 205.11(b) and (c).

[35] *Id.*

[36] 15 U.S.C. 1693f(b).

[37] 15 U.S.C. 1693f(c), 12 C.F.R. 205.11(c).

[38] For a list of state identity theft statutes see [http://www.consumer.gov/idtheft/federallaws.html#statelaws].

[39] Cal. Penal Code §§ 530.5 - 530.7.

[40] Tex. Penal Code § 32.51. *See also* Va. Code Ann. § 18.2-186.3; Md. Code Ann. art. 27 § 231.

[41] RCW 9.35.020(3).

obtains or attempts to obtain is $750 or more."[42] In Illinois, the crime of financial identity theft includes the fraudulent use of credit card numbers, in addition to the fraudulent use of identification documents.[43]

State Laws Aimed at Assisting Victims. In addition to the states that provide for criminal prosecution of impostors, some states have enacted laws aimed at assisting victims of identity theft. These laws served as a model for the recently enacted Fair and Accurate Credit Transactions (FACT) Act's amendments to the FCRA. Pursuant to amendments made by the FACT Act, many of these provisions are now preempted by federal law, subject to certain exceptions and exclusions.[44]

Prior to the enactment of the federal law, at least three states – California, Idaho, and Washington – enacted laws allowing victims of identity theft to place fraud alerts on their credit reports or have information resulting from the alleged theft blocked from their credit reports.[45]

California enacted what some consider to be the most extensive law aimed at assisting victims of identity theft and preventing future occurrences. Under California law, a consumer may request that a security alert be placed in his or her credit report to notify recipients of the 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."[46] Consumer reporting agencies are required to notify each person requesting consumer credit information with respect to a consumer of the existence of a security alert in the consumer's report, regardless of whether a full credit report, credit score, or summary report is requested.[47]

A consumer may also be able to have a security freeze placed on his or her credit report by making a request in writing by certified mail with a consumer credit reporting agency.[48] A security freeze prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.[49] The consumer reporting agency may advise a third party requesting the consumer's report that a security freeze is in place, but may not release any additional information without prior express authorization from the consumer. If a security freeze is in place, a consumer credit reporting agency may not change the name, date of birth, social security number, or address in a consumer

---

[42] Or. Rev. Stat. § 165.055.

[43] 720 ILCS 5/16G-10. *See also* Ohio Rev. Code Ann. § 2913.49.

[44] For more information on the FCRA's preemption of state law, see CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law.*

[45] California, Cal. Civ. Code § 1785.11.1; Idaho, Idaho Code § 28-51-02; Washington, RCW 19.182.160.

[46] Cal. Civ. Code § 1785.11.1(a).

[47] Cal. Civ. Code § 1785.11.1(b).

[48] Cal. Civ. Code § 1785.11.2(a).

[49] *Id.*

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.[50] In the case of an address change, the written confirmation must be sent to both the new address and to the former address.

Victims of identity theft who are sued on an obligation resulting from the theft, may bring a cross-claim alleging identity theft. If the victim prevails, he or she is entitled to a judgment stating that he or she is not responsible for the debt or other basis for the claim and an injunction restraining any collection efforts.[51] The victim may join other claimants, and the court may keep jurisdiction for up to ten years, so as to resolve all claims resulting from the theft.

An additional provision, required a consumer reporting agency to provide consumers who have reason to believe that they are victims of identity theft with information as to their rights under California law.[52] Upon receipt from a victim of identity theft of a police report or a valid investigative report, a consumer reporting agency must also provide a victim of identity theft with up to 12 copies of his or her credit report during a consecutive 12-month period free of charge.[53]

Washington has also enacted an extensive identity theft statute that includes provisions aimed at assisting victims of identity theft. As noted above, the Washington identity theft statute has a provision that allows consumers to block information resulting from identity theft from their credit reports. A consumer reporting agency must block such information within 30 days of receiving a copy of a police report regarding the alleged theft.[54] Another provision allows victims of identity theft to receive information about the alleged crime from persons who may have entered into transactions with the impostor. Upon the request of the victim, such persons must provide copies of all relevant application and transaction information related to the alleged fraudulent transaction.[55]

Federal Legislation

Several bills related to identity theft have been introduced during the 109th Congress. Some of this legislation (S. 500, S. 751, S. 768 and H.R. 1080) was introduced in response to the announcement by major information brokerage firms that their systems had been compromised leading to the unauthorized disclosure of consumer information.[56] These bills are included in the list provided below.

---

[50] Cal. Civ. Code § 1785.11.3(a).

[51] Cal. Civ. Code § 1798.2.

[52] Cal. Civ. Code § 1785.15.3(a).

[53] Cal. Civ. Code § 1785.15.3(b).

[54] RCW 19.182.160.

[55] RCW 9.35.040.

[56] For more information on federal and state laws applicable to information brokers, see CRS Report RS22087, *Information Brokers: Federal and State Laws*. *See also* CRS Report (continued...)

H.R. 1263, the **Consumer Privacy Protection Act of 2005**, would, *inter alia*, require the Federal Trade Commission to take certain actions with respect to identity theft prevention and victim's assistance. The Commission would be required to take such action as may be necessary to permit consumers that have a reasonable belief that they are a victim of identity theft to complete a Commission-developed document entitled "Identity Theft Affidavit" and submit the document and other supplemental information to the Commission and other entities. The Commission would be required to solicit the acceptance and acknowledgment of the affidavit by entities that receive disputes regarding the unauthorized use of accounts of such entities from consumers who have reason to believe that they are victims of identity theft. The Commission would also be required to require such entities to conduct any necessary investigation and decide the outcome of a claim within 90 days from the date on which all necessary information has been submitted to the entity. The legislation would also require the Commission to require entities to take reasonable steps to verify the accuracy of a consumer's address, including by confirming changes of address by sending confirmation of the change to the old and new address.

H.R. 1099, the **Anti-phishing Act of 2005**, would make it a federal crime to knowingly, with the intent to carry on any activity which would be a federal or state crime of fraud or identity theft, create or procure the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate online business; and use that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another. It would also be a crime to send a message that falsely represents itself as being sent by a legitimate online business for the purposes listed above. The penalty for each could be a fine, imprisonment for five years, or both. A substantially similar bill, **S. 472**, was introduced in the Senate.

H.R. 1078, the **Social Security Number Protection Act of 2005**, would direct the Federal Trade Commission to promulgate regulations to impose restrictions and conditions on the sale and purchase of social security numbers, subject to certain exceptions.

H.R. 220, the **Identity Theft Prevention Act of 2005**, would repeal provisions of the Social Security Act authorizing various uses of the social security number. The bill would also require all social security numbers to be randomly generated, make the social security number the property of the individual to whom it is issued, and prohibit the Social Security Administration from disclosing the number to any agency or instrumentality of the federal or state government. The federal government would also be prohibited from issuing government-wide identifying numbers or establishing a uniform standard for identification of an individual that is required to be used by any other federal agency, state agency, or private person.

S. 768, the **Comprehensive Identity Theft Prevention Act**, includes a number of provisions aimed at preventing identity theft, including the creation of an Office

---

[56] (...continued)
RS22082, *Identity Theft: The Internet Connection.*

of Identity Theft in the Federal Trade Commission and efforts to protect a consumer's sensitive personal information. The bill would require the Federal Trade Commission to promulgate regulations to enable the newly created Office of Identity Theft to protect sensitive personal information that is collected, maintained, sold, or transferred by commercial entities, such as information brokers. The Office of Identity Theft would also assist consumers who have been victims of identity theft. Information brokers, or data merchants, as defined in the legislation, would be required to register with the Office of Identity Theft, and would be required to follow rules promulgate by the Commission regarding the processes for protecting consumer information. Consumers would be given certain rights, similar to those afforded under the Fair Credit Reporting Act, with respect to their information held by a data merchant, and would be able to correct incorrect information and receive one free report from the data merchant each year. Commercial entities would be required to notify consumers of information breaches, and consumers would be able to have their information expunged from the information broker's records following notification of a security breach. The bill would also place limitation on the sale, purchase, display and use of social security numbers and create an Office of Cybersecurity in the Department of Homeland Security.

S. 751, the **Notification of Risk to Personal Data Act**, would require, following the discovery of a security breach, "any agency, or person engaged in interstate commerce, that owns, licenses, or collects data, whether or not held in electronic form, containing personal information" to notify individuals whose information may have been acquired by an unauthorized person. The notification must be made "without unreasonable delay" following the discovery of the security breach, but may be delayed if a law enforcement agency determines that the notification would seriously impede a criminal investigation.

S. 500, the **Information Protection and Security Act** would require the Federal Trade Commission to promulgate regulations "with respect to the conduct of information brokers and the protection of personally identifiable information held by such brokers." Such regulations must include a requirement that procedures for the collection and maintenance of data guarantee maximum possible accuracy of the information held by brokers; access by a consumer to information pertaining to him held by an information broker; a consumer's right to request and receive prompt correction of errors in information held by an information broker; a requirement that brokers safeguard and protect the confidentially of information; a requirement that brokers authenticate users before allowing access to information and that the broker ensure that the information will only be used for a lawful purpose; and a requirement that broker's establish procedures to prevent and detect fraudulent or unlawful access, use or disclosure of information. A companion bill, **H.R. 1080**, was introduced in the House.

S. 116, the **Privacy Act of 2005**, while not specifically aimed at preventing identity theft, includes a number of privacy provisions that could aid in preventing the disclosure of information that could be used by identity thieves. The bill would, *inter alia*, place restrictions and limitations on the collection and dissemination of personally identifiable information; prohibit the display, sale, or purchase of social security numbers; place limits on the disclosure of social security numbers for

consumer transactions; place limits on the sale and sharing of nonpublic personal information; and place limits on the provision of protected health information.

S. 115, the **Notification of Risk to Personal Data Act** would require "any agency, or person engaged in interstate commerce, that owns or licenses electronic data containing personal information" to "notify any resident of the United States whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a security breach. Notification would be required "as expediently as possible and without unreasonable delay" following the discovery of the breach of security and any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the integrity of the data system.

S. 29, the **Social Security Number Misuse Prevention Act**, would place restrictions and limitations on the display, sale and purchase of the social security number under a variety of circumstances.