Order Code RL31919

Remedies Available to Victims of Identity Theft

Updated September 12, 2003

Angie A. Welborn
Legislative Attorney
American Law Division

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 three consecutive years.[1] 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. State laws and recent legislative proposals (S. 22, S. 153, S. 223, S. 228, S. 745, S. 1533, S. 1581, H.R. 220, H.R. 637, H.R. 818, H.R. 858, H.R. 1636, H.R. 1729, H.R. 1731, H.R. 1931, H.R. 2035, 2617, H.R. 2622, H.R. 2633, and H.R. 2971) aimed at preventing identity theft and providing additional remedies are also discussed. This report will be updated as events warrant.

[1][http://www.consumer.gov/sentinel/trends.htm].

Contents

Federal Statutes Related to Identity Theft 1
Identity Theft Assumption and Deterrence Act 1
Fair Credit Reporting Act 2
Fair Credit Billing Act 3
Electronic Fund Transfer Act 3
State Identity Theft Statutes 4
State Criminal Laws 4
State Laws Aimed at Assisting Victims 5
Legislative Proposals 6
107th Congress 6
108th Congress 6

Remedies Available to Victims of Identity Theft

Federal Statutes 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.[2] 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,[3] to knowingly and without lawful authority produce an identification document[4] 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.[5] 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

---

[2]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.

[3]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).

[4]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.

[5]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.[6]

The punishment for offenses involving fraud related to identification documents varies depending on the specific offense and the type of document involved.[7] 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.[8] Other offenses carry terms of imprisonment up to three years.[9] 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.[10] Offenses committed to facilitate an action of international terrorism are punishable by terms of imprisonment up to twenty-five years.[11]

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. 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."[12] 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 requires credit reporting agencies to follow "reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."[13]

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.[14] 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

---

[6]18 U.S.C. 1028(a)(7).

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

[8]18 U.S.C. 1028(b)(1)(D).

[9]18 U.S.C. 1028(b)(2).

[10]18 U.S.C. 1028(b)(3).

[11]18 U.S.C. 1028(b)(4).

[12]15 U.S.C. 1681(b).

[13]15 U.S.C. 1681e(b).

[14]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*.

information as a result of the consumer's stolen identity. Generally, the FCRA requires a consumer to file suit "within two years from the date on which the liability arises."[15] However, there is an exception in cases where there was willful misrepresentation of information that is required to be disclosed to a consumer and such information is material to the establishment of the defendant's liability.[16] In such cases, the action "may be brought any time within two years after the discovery by the individual of the misrepresentation."[17]

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."[18] 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.[19]

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.[20] 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.[21]

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."[22] 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

---

[15] 15 U.S.C. 1681p.

[16] *Id.*

[17] *Id.*

[18] 15 U.S.C. 1601(a).

[19] 15 U.S.C. 1666(b); 12 C.F.R. 226.13(a).

[20] 15 U.S.C. 1666(c); 12 C.F.R. 226.13(d)(1).

[21] 15 U.S.C. 1666(a); 12 C.F.R. 226.13(e).

[22] 15 U.S.C. 1693(b).

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.[23]

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 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.[24] 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.[25]

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.[26] 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.[27]

State Identity Theft Statutes

State Criminal Laws. Most states have enacted some type of criminal identity theft statute.[28] 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.[29] 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.[30] 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

---

[23]15 U.S.C. 1693g(a), 12 C.F.R. 205.6(b)(1).

[24]15 U.S.C. 1693f(a), 12 C.F.R. 205.11(b) and (c).

[25]*Id.*

[26]15 U.S.C. 1693f(b).

[27]15 U.S.C. 1693f(c), 12 C.F.R. 205.11(c).

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

[29]Cal. Penal Code §§ 530.5 - 530.7.

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

damages of five hundred dollars or actual damages, whichever is greater, including costs to repair the victim's credit record."[31]

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 obtains or attempts to obtain is $750 or more."[32] 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.[33]

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. At least three states – California, Idaho, and Washington – have enacted laws allowing victims of identity theft place fraud alerts on their credit reports or have information resulting from the alleged theft blocked from their credit reports.[34]

California has 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."[35] 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.[36]

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.[37] 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.[38] 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

---

[31]RCW 9.35.020(3).

[32] Or. Rev. Stat. § 165.055.

[33]720 ILCS 5/16G-10. *See also* Ohio Rev. Code Ann. § 2913.49.

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

[35]Cal. Civ. Code § 1785.11.1(a).

[36]Cal. Civ. Code § 1785.11.1(b).

[37]Cal. Civ. Code § 1785.11.2(a).

[38]*Id.*

not change the name, date of birth, social security number, or address 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.[39] 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.[40] 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.

A new provision which became effective July 1, 2003, requires 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.[41] 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.[42]

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.[43] 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.[44]

Legislative Proposals

107th Congress. During the 107th Congress, numerous bills related to identity theft were introduced. An overview of this legislation can be found in CRS Report RL31752, *Identity Theft: An Overview of Proposed Legislation*.

108th Congress. To date, a number of bills related to identity theft have been introduced in the 108th Congress. With the exception of S. 153, which was passed

---

[39]Cal. Civ. Code § 1785.11.3(a).

[40]Cal. Civ. Code § 1798.2.

[41]Cal. Civ. Code § 1785.15.3(a).

[42]Cal. Civ. Code § 1785.15.3(b).

[43]RCW 19.182.160.

[44]RCW 9.35.040.

by the Senate, without amendment, on March 19, and H.R. 2622, which was passed by the House on September 10, no additional action has been taken on this legislation, though both the House and the Senate have held hearings on identity theft and financial privacy. In general, these bills include provisions similar to those found in legislation introduced during the 107th Congress.

Title III of **S. 22**, the **Justice Enhancement and Domestic Security Act of 2003**, includes several provisions aimed at deterring and preventing identity theft, including identity theft mitigation, amendments to the Fair Credit Reporting Act requiring the blocking of information on a consumer's credit report resulting from identity theft, an amendment to the FCRA's statute of limitations, provisions related to the misuse of social security numbers, and prevention provisions similar to those in S. 223 discussed below.

S. 153, the **Identity Theft Penalty Enhancement Act**, would amend Title 18 of the United States Code to establish penalties for aggravated identity theft and make changes to the existing identity theft provisions of Title 18. Under S. 153, aggravated identity theft would occur 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. The penalty for aggravated identity theft would be a term of imprisonment of 2 years in addition to the punishment provided for the original felony committed. Offenses committed in conjunction with certain terrorism offenses would be subject to an additional term of imprisonment of 5 years. **H.R. 858** and **H.R. 1731** appear to be substantially similar.

S. 223, the **Identity Theft Prevention Act**, includes several provisions aimed at preventing identity theft, including a requirement that credit card issuers confirm change of address requests, a requirement that consumer reporting agencies include fraud alerts in consumer reports at the request of the consumer, and a requirement that credit card numbers on printed receipts be truncated.

S. 228, the **Social Security Number Misuse Prevention Act**, would prohibit the display, sale, or purchase of an individual's social security number with limited exceptions. It would also prohibit the display, sale, or purchase of public records containing social security numbers, and prohibit the use of social security numbers on certain government documents, such as checks and driver's licenses. The bill would also place limitations on the use of social security numbers by commercial entities. **H.R. 637** appears to be substantially similar.

S. 745, the **Privacy Act of 2003**, while not directly related to identity theft, includes numerous provisions aimed at protecting the privacy of personal information, which could assist identity theft prevention efforts. Provisions set forth in S. 745 would generally prohibit the collection and distribution of personally identifiable information unless the individual receives notification and is provided an opportunity to restrict the disclosure or sale of such information; prohibit the display, sale, or purchase of an individual's Social Security number without consent from the individual; place limitations on the sale and sharing of nonpublic personal financial information; place limitations on the provisions of protected health

information; and prohibit the release of certain information included on an individual's driver's license.

S. 1533, the **Identity Theft Victims Assistance Act of 2003**, includes a number of provisions aimed at assisting victims of identity theft. The bill would require businesses that possess information relating to an alleged identity theft to provide the alleged victim or a law enforcement agency authorized by the victim with such information no later than 20 days after receiving a request from the victim and upon verification of the victim's identity. The bill would also amend the Fair Credit Reporting Act to allow victims of identity theft to block information resulting from the theft from their credit reports and to extend the FCRA's statute of limitations. **S. 1581** appears to include similar provisions.

H.R. 220, the **Identity Theft Prevention Act of 2003**, would place new restrictions on the use of social security numbers and require all social security numbers to be randomly generated.

H.R. 818, the **Identity Theft Consumer Notification Act**, would require financial institutions to notify consumers whose personal information has been compromised. The financial institution would also be required to assist the individual by correcting information in the consumer's credit file and to compensate the consumer for any monetary losses resulting from the compromise. The bill would also amend the Fair Credit Reporting Act's statute of limitations to allow additional time for a consumer to file suit.

H.R. 1636, the **Consumer Privacy Protection Act of 2003**, includes several provisions aimed at protecting consumer privacy. Title I of the bill addresses a consumer's rights with respect to the use or dissemination of his or her personal information in interstate commerce, including a requirement that consumers be given an opportunity to preclude the sale or disclosure of the consumer's personally identifiable information. Title II specifically addresses the prevention of identity theft and provides remedies for victims of identity theft. The bill would require the Federal Trade Commission to take actions necessary to permit consumers to file electronic identity theft affidavits with the Commission and to promote the use of a common identity theft affidavit among entities that receive disputes regarding the unauthorized use of accounts from consumers that have reason to believe that they are victims of identity theft. The legislation also directs the FTC to require such entities to resolve identity theft disputes within 90 days from the date on which all necessary information to investigate the claim has been submitted. The bill would also make improvements to the Commission's consumer clearinghouse, and require the collection of data from public and private entities that receive and process complaints from consumers that have a reasonable belief that they are victims of identity theft.

H.R. 1729, the **Negative Credit Notification Act**, would require a consumer reporting agency to notify a consumer if any information that is, or may be construed as being, adverse to the interests of the consumer is added to the consumer's file. The notification must also include a brief description of the information "sufficient to allow the consumer to determine the accuracy or completeness of the information so furnished and the source of the information."

H.R. 1931, the **Personal Information Privacy Act of 2003**, includes several provisions aimed at protecting an individual's Social Security number and other personal information. The bill would amend the Fair Credit Reporting Act to include in the definition of a consumer report any identifying information of the consumer, except the name, address and telephone number of the consumer if listed in a residential telephone directory available in the locality of the consumer, and require a consumer reporting agency to receive express written authorization from a consumer prior to releasing information with respect to a transaction that was not initiated by the consumer. An additional amendment to the FCRA would add a new section prohibiting the sale or transfer of transaction or experience information without the consumer's express written consent. H.R. 1931 would also prohibit the use of an individual's Social Security number for commercial purposes without consent.

H.R. 2035, the **Identity Theft and Financial Privacy Act of 2003**, includes several provisions aimed at preventing identity theft. The bill would require credit card issuers to confirm change of address requests if such request is received within 30 days of a request for an additional card, and amend the Fair Credit Reporting Act to require consumer reporting agencies to notify requesters of potential fraud when the request includes an address for the consumer that is substantially different from the most recent address on file with the consumer reporting agency. An additional amendment to the FCRA would require consumer reporting agencies, upon receipt of proper identification, to include a fraud alert in a consumer's file if the consumer has been or suspects that he or she is about to become a victim of identity theft. The consumer reporting agency would be required to notify each person procuring the consumer's file of the existence of a fraud alert, regardless of whether a full credit report, credit score, or summary report is requested. The Federal Trade Commission would be required to promulgate rules providing for procedures for referral of consumer complaints about identity theft and fraud alters between and among the consumer reporting agencies and the Commission. In addition, rules developing a model form and standard procedures to be used by consumers who are victims of identity theft for contacting and informing creditors and consumer agencies of the fraud would be required. H.R. 2035 would also require the truncation of credit card numbers on printed receipts and require consumer reporting agencies to provide free credit reports annually upon the request of a consumer.

H.R. 2617, the **Consumer Identity and Information Security Act of 2003**, includes several provisions aimed at preventing identity theft and assisting victims. The bill would prohibit certain actions with respect to an individual's social security number, including prohibitions on the display of an individual's social security number and a prohibition on requiring an individual to transmit his or her social security number over the Internet. The truncation of credit and debit card numbers on receipts would also be required. The bill would also require credit card issuers to verify a consumer's identity if the issuer receives a change of address request within 30 days of receiving a request for an additional card. Consumer reporting agencies would also be required, upon receipt of proper identification, to include in a consumer's file a fraud alert and notify all subsequent users of the consumer's report of the existence of the alert. A consumer reporting agency that maintains files on a nationwide basis would be required to notify other such agencies of the alert, and such agencies would then be required to place similar alerts in the files they maintain.

H.R. 2622, the **Fair and Accurate Credit Transactions Act of 2003**, as passed by the House on September 10, includes, *inter alia*, several provisions aimed at preventing identity theft and assisting victims of identity theft. The bill would amend the Fair Credit Reporting Act to require credit card issuers to investigate change of address requests if the issuer receives a request for an additional credit card within 30 days of receiving notification of a change of address. Another amendment to the FCRA would require consumer reporting agencies to include fraud alerts in a consumer's file upon the request of the consumer. Once included, the agency would be required to notify each person procuring the report of the existence of the alert. Consumer reporting agencies would also be required to reconcile differences in addresses when the consumer reporting agency receives a request for a report that includes an address that substantially differs from the one the agency has on file. The bill would also require the truncation of credit card and debit card account numbers.

Provisions aimed at assisting victims include an amendment to the FCRA which would require the Federal Trade Commission to develop a model summary of the rights of consumers with respect to the procedures for remedying the effects of fraud or identity theft involving credit, electronic fund transfers, or accounts or transactions at or with a financial institution. Consumer reporting agencies would be required to provide a consumer who contacts the agency expressing a belief that he or she is a victim of identity theft with the summary of rights developed by the FTC. An additional amendment to the FCRA would require consumer reporting agencies, after receipt of proof of identity of the consumer and an official copy of the policy report, to block any information identified by the consumer in the consumer's file as resulting from the alleged identity theft. Additionally, the bill would require the federal banking agencies to jointly establish and maintain guidelines for use in identifying patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

H.R. 2633, the **Identity Theft Protection and Information Blackout Act of 2003**, includes a number of provisions restricting the sale, purchase, display, and use of an individual's social security number in both the government and private sector. The bill would also deem the refusal to do business without receipt of a social security number an unfair or deceptive act of practice under the Federal Trade Commission Act, and prohibit the disclosure of a social security number by a consumer reporting agency except in connection with the disclosure of a full consumer credit report furnished in accordance with section 604 of the FCRA. H.R. 2633 also includes provisions aimed at protecting the privacy of medical information in connection with financial transactions, and prohibiting the use of medical information in connection with any decision to offer, provide, or continue to provide any financial product or service.

H.R. 2971, the **Social Security Number Privacy and Identity Theft Prevention Act of 2003**, includes a number of provisions aimed at restricting or prohibiting the use of social security account numbers in the private and public sectors. In general, these provisions are similar to those found in other bills discussed *supra*.