Order Code RL31919

CRS Report for Congress

Federal Laws Related to Identity Theft

Updated January 30, 2008

Gina Marie Stevens
Legislative Attorney
American Law Division

Prepared for Members and
Committees of Congress

Federal Laws Related to 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 seven 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. This report will be updated as events warrant.

Contents

Federal Laws Related to Identity Theft

Introduction[1]

According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all 50 states, and accounts for over 35% of the total number of complaints the Identity Theft Data Clearinghouse received for calendar years 2004, 2005, and 2006. In calendar year 2006, of the 674,354 complaints received, 246,035 or 36% were identity theft complaints.[2] The identity theft victim's information was misused for credit card fraud in 25% of the identity theft complaints; for phone or utilities fraud in 16% of the identity theft complaints; for bank fraud in 16% of the identity theft complaints; for employment-related fraud in 14% of the identity theft complaints; for government documents or benefits fraud in 5% of the identity theft complaints; for loan fraud in 5% of the identity theft complaints; and other types of identity theft fraud made up 24% of the complaints.

As a result of identity theft, victims may incur damaged credit records, unauthorized charges on credit cards, and unauthorized withdrawals from bank accounts.[3] 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. With media reports of data security breaches increasing, concerns about new cases of identity theft are widespread.[4]

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.[5] This report will be updated as warranted.

---

[1] This report was originally prepared by Angie A. Welborn, Legislative Attorney.

[2] Federal Trade Commission, *Identity Theft Victim Complaint Data*, Feb. 7, 2007, at [http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf].

[3] See Nancy Trejos, "*Identity Theft Gets Personal: When a Debit Card Number Is Stolen, America's New Crime Wave Hits Home*," Washington Post at F01 (Jan. 13, 2008).

[4] Legislation that has been introduced in response to the increase in information security breaches is discussed in CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens.

[5] For information on state identity theft laws, see National Conference of State Legislators, Identity Theft Statutes & Criminal Penalties, at [http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm].

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.[6] 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,[7] to knowingly and without lawful authority produce an identification document,[8] authentication feature ,[9] or false identification document;[10] 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

---

[6] 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.

[7] 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).

[8] 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)(3). Identification documents include Social Security cards, birth certificates, driver's licenses, and personal identification cards.

[9] Authentication feature is defined as "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." 18 U.S.C. 1028(d)(1).

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

produced without such authority.[11] It is also a federal crime to knowingly transfer or use, without lawful authority, a means of identification[12] of another person with the intent to commit, or 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.[13]

The punishment for offenses involving fraud related to identification documents varies depending on the specific offense and the type of document involved.[14] 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.[15] Other offenses carry terms of imprisonment up to three years.[16] 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.[17] Offenses committed to facilitate an action of international terrorism are punishable by terms of imprisonment up to twenty-five years.[18]

Identity Theft Penalty Enhancement Act. The Identity Theft Penalty Enhancement Act was signed 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 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.[19]

---

[11] 18 U.S.C. 1028(a)(1) and (2).

[12] Means of identification is defined 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))." 18 U.S.C. 1028(d)(7).

[13] 18 U.S.C. 1028(a)(7).

[14] 18 U.S.C. 1028(b).

[15] 18 U.S.C. 1028(b)(1)(D).

[16] 18 U.S.C. 1028(b)(2).

[17] 18 U.S.C. 1028(b)(3).

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

[19] 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;

(continued...)

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.[20]

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."[21]

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.[22] 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."[23] 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.[24] 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

---

[19] (...continued)
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).

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

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

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

[23] 15 U.S.C. 1681(b).

[24] 15 U.S.C. 1681n; 15 U.S.C. 1681o.

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.[25]

Fair and Accurate Credit Transactions (FACT) Act of 2003. The FACT Act, signed 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.[26] Generally, these new provisions mirror laws passed by state legislatures and create a national standard for addressing consumer concerns with regard to identity theft and other types of fraud.[27]

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.[28] In a further effort to prevent identity theft, other new provisions require the truncation of credit card account numbers on electronically printed receipts,[29] and, upon request, the truncation of social security numbers on credit reports provided to a consumer.[30]

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.[31] 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.[32]

In addition to the fraud alert, victims of identity theft may also have information resulting from the crime blocked from their credit reports.[33] 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

---

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

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

[27] 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*, by Angie A. Welborn.

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

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

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

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

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

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

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.[34]

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 or to any law enforcement agency investigating the theft and authorized by the victim to take receipt of the records in question.[35]

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."[36] 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.[37]

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.[38] 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.[39]

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,

---

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

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

[36] 15 U.S.C. 1601(a).

[37] 15 U.S.C. 1666(b); 12 C.F.R. 226.13(a).

[38] 15 U.S.C. 1666(c); 12 C.F.R. 226.13(d)(1).

[39] 15 U.S.C. 1666(a); 12 C.F.R. 226.13(e).

liabilities, and responsibilities of participants in electronic fund transfer systems."[40] 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.[41]

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 10 business days.[42] 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.[43]

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.[44] 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 10 business days.[45]

Identity Theft Task Force

The President's Identity Theft Task Force reported its final recommendations April 2007, and recommended a plan that is intended to harness government resources to crack down on the criminals who traffic in stolen identities, strengthen efforts to protect the personal information, help law enforcement officials investigate and prosecute identity thieves, help educate consumers and businesses about protecting themselves, and increase the safeguards on personal data entrusted to federal agencies and private entities.[46] The Plan focuses on improvements in four key areas: keeping sensitive consumer data from identity thieves through better data

---

[40] 15 U.S.C. 1693(b).

[41] 15 U.S.C. 1693g(a), 12 C.F.R. 205.6(b)(1).

[42] 15 U.S.C. 1693f(a), 12 C.F.R. 205.11(b) and (c).

[43] *Id.*

[44] 15 U.S.C. 1693f(b).

[45] 15 U.S.C. 1693f(c), 12 C.F.R. 205.11(c).

[46] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007 at [http://www.identitytheft.gov/reports/StrategicPlan.pdf].

security and education; making it more difficult for identity thieves who obtain consumer data; assisting the victims of identity theft in recovering from the crime; and deterring identity theft by more aggressive prosecution and punishment. Several recommendations made by the Task Force are aimed at closing the gaps in federal criminal statutes used to prosecute identity theft-related offenses to ensure increased federal prosecution. They are as follows:[47]

- Amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted
- Add new crimes to the list of predicate offenses for aggravated identity theft offenses
- Amend the statute that criminalizes the theft of electronic data by eliminating the current requirement that the information must have been stolen through interstate communications
- Penalize creators and distributors of malicious spyware and keyloggers
- Amend the cyber-extortion statute to cover additional, alternate types of cyber-extortion
- Ensure that an identity thief's sentence can be enhanced when the criminal conduct affects more than one victim

Real ID

In accordance with the REAL ID Act of 2005, on January 11, 2008, the Department of Homeland Security (DHS) published the final rule for State-issued driver's licenses and identification cards that federal agencies would accept for official purposes on or after May 11, 2008, in accordance with the REAL ID Act of 2005. [48] The Real ID Rule establishes standards to meet the minimum requirements of the REAL ID Act.[49] These standards involve a number of aspects of the process used to issue identification documents, including information and security features that must be incorporated into each card; proof of identity and U.S. citizenship or legal status of an applicant; verification of the source documents provided by an applicant; and security standards for the offices that issue licenses and identification cards. All states submitting requests will receive extensions until December 31, 2009. In addition, states that meet certain benchmarks for the security of their credentials and licensing and identification processes will be able to obtain a second extension until May 10, 2011. The Rule extends the enrollment time period to allow states determined by DHS to be in compliance with the act to replace all licenses intended for official purpose with REAL ID-compliant cards by December 1, 2014, for people born after December 1, 1964, and by December 1, 2017, for those born on or before December 1, 1964. The rule is effective March 31, 2008.

---

[47] *Id.* at 4.

[48] 73 F.R. 5271 (Jan. 29, 2008).

[49] See Department of Homeland Security, REAL ID Final Rule: Questions & Answers at [http://www.dhs.gov/xprevprot/programs/gc_1172767635686.shtm].