Identity Theft: Trends and Issues

Kristin M. Finklea
Specialist in Domestic Security

December 14, 2011

Congressional Research Service
7-5700
www.crs.gov
R40599

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

In the current fiscal environment, policymakers are increasingly concerned with securing the economic health of the United States—including combating those crimes that threaten to further undermine the nation's financial stability. Identity theft is one such crime. In 2010, about 8.1 million Americans were reportedly victims of identity fraud, and the average identity fraud victim incurred a mean of $631 in costs as a result of the fraud—the highest level since 2007. Identity theft is often committed to facilitate other crimes such as credit card fraud, document fraud, or employment fraud, which in turn can affect not only the nation's economy but its security. Consequently, in securing the nation and its economic health, policymakers are also tasked with reducing identity theft and its impact.

Identity theft has remained the dominant consumer fraud complaint to the Federal Trade Commission (FTC). Nevertheless, while the number of overall identity theft complaints generally increased between when the FTC began recording identity theft complaints in 2000 and 2008, the number of complaints decreased in both 2009 and 2010. Prosecutions of federal identity theft violations have followed a similar pattern. However, while the number of identity theft cases filed and the number of defendants convicted both decreased in FY2009 and FY2010 relative to FY2008, the numbers of *aggravated* identity theft cases filed and defendants convicted have continued to increase.

Congress continues to debate the federal government's role in (1) preventing identity theft and its related crimes, (2) mitigating the potential effects of identity theft after it occurs, and (3) providing the most effective tools to investigate and prosecute identity thieves. With respect to preventing identity theft, one issue concerning policymakers is the prevalence of personally identifiable information—and in particular, the prevalence of Social Security numbers (SSNs)—in both the private and public sectors. One policy option to reduce their prevalence may involve restricting the use of SSNs on government-issued documents such as Medicare identification cards. Another option could entail providing federal agencies with increased regulatory authority to curb the prevalence of SSN use in the private sector. In debating policies to mitigate the effects of identity theft, one option Congress may consider is whether to strengthen data breach notification requirements. Such requirements could affect the notification of relevant law enforcement authorities as well as any individuals whose personally identifiable information may be at risk from the breach.

There have already been several legislative and administrative actions aimed at curtailing identity theft. Congress enacted legislation naming identity theft as a federal crime in 1998 (P.L. 105-318) and later provided for enhanced penalties for aggravated identity theft (P.L. 108-275). In April 2007, the President's Identity Theft Task Force issued recommendations to combat identity theft, including specific legislative recommendations to close identity theft-related gaps in the federal criminal statutes. In a further attempt to curb identity theft, Congress directed the FTC to issue an Identity Theft Red Flags Rule (effective December 31, 2010), requiring that creditors and financial institutions with specified account types develop and institute written identity theft prevention programs.

Contents

Introduction 1
Definitions of Identity Theft 2
Theft vs. Fraud 3
Knowledge Element 3
Legislative History 3
Identity Theft Assumption Deterrence Act 4
Identity Theft Penalty Enhancement Act 4
Identity Theft Enforcement and Restitution Act of 2008 4
Identity Theft Task Force 5
Recommendations 5
Legislative Recommendations 6
Red Flags Rule 7
Trends in Identity Theft 9
Perpetrators 11
Investigations and Prosecutions 12
Federal Bureau of Investigation (FBI) 13
United States Secret Service (USSS) 13
United States Postal Inspection Service (USPIS) 13
Social Security Administration Office of the Inspector General (SSA OIG) 14
Immigration and Customs Enforcement 14
Department of Justice 14
Domestic Impact 17
Credit Card Fraud 19
Document Fraud 19
Employment Fraud 20
Data Breaches and Identity Theft 20
Potential Issues for Congress 23
Identity Theft Prevention 23
Securing Social Security Numbers 24
Effects of Data Breaches 25
Deterrence and Punishment 26
Selected Legislation from the 112th Congress 27
Social Security Numbers 27
Law Enforcement and Consumer Notification 27

Figures

Figure 1. FTC Consumer Complaint Data 10
Figure 2. FTC Identity Theft Complaint Data 11
Figure 3. Federal Identity Theft and Aggravated Identity Theft Cases 16
Figure 4. FTC Identity Theft Complaints, 2010 18
Figure 5. Total Number of Reported Data Breaches and Records Affected 21

Contacts

Author Contact Information..... 28

Introduction

In the current fiscal environment, policymakers are increasingly concerned with securing the economic health of the United States—including combating those crimes that threaten to further undermine the nation's financial stability.[1] Identity theft, for one, poses both security and economic risks. By some estimates, identity fraud cost Americans $37 billion in 2010.[2] FTC complaint data indicate that the most common fraud complaint received (19% of all consumer fraud complaints) is that of identity theft.[3] In 2010, for instance, about 8.1 million Americans were reportedly victims of identity fraud. This is a decrease of about 3 million from the approximately 11.1 million who were victimized in 2009.[4] Despite this decline in the overall number of reported identity fraud incidents, difficulty in detecting and resolving these incidents may have contributed in higher consumer costs; the average identity fraud victim incurred a mean of $631—the highest level since 2007.[5]

An increase in globalization and a lack of cyber borders provide an environment ripe for identity thieves to operate from within the nation's borders—as well as from beyond. Federal law enforcement is thus challenged with investigating criminals who may or may not be operating within U.S. borders; may have numerous identities—actual, stolen, or cyber; and may be acting alone or as part of a sophisticated criminal enterprise.[6] In addition, identity theft is often interconnected with various other criminal activities. These activities range from credit card and bank fraud to immigration and employment fraud. In turn, the effects felt by individuals and businesses who have fallen prey to identity thieves extend outside of pure financial burdens; identity thieves affect not only the nation's economic health, but its national security as well. Consequently, policymakers may debate the federal government's role in preventing identity theft and its related crimes, mitigating the potential effects of identity theft after it occurs, and providing the most effective tools to investigate and prosecute identity thieves.

This report first provides a brief federal legislative history of identity theft laws. It analyzes the current trends in identity theft, including prevalent identity theft-related crimes, the federal agencies involved in combating identity theft, and the trends in identity theft complaints and prosecutions. The report also discusses the relationship between data breaches and identity theft as well as possible effects of the FTC's Identity Theft Red Flags Rule, effective December 31, 2010. It also examines possible issues for Congress to consider.

[1] See, for example, U.S. Congress, House Committee on Ways and Means, *Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy*, 112th Cong., 1st sess., April 13, 2011.

[2] Javelin Strategy & Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011.

[3] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December, 2010*, March, 2011, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

[4] Javelin Strategy & Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011.

[5] Ibid.

[6] For more information on these challenges, see CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin M. Finklea.

Definitions of Identity Theft

When does taking and using someone else's identity become a crime? Current federal law defines identity theft as a federal crime when someone

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

The current federal law also provides enhanced penalties for *aggravated identity theft* when someone "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" in the commission of particular felony violations.[8] Aggravated identity theft carries an enhanced two-year prison sentence for most specified crimes and an enhanced five-year sentence for specified terrorism violations.

Identity theft is also defined in the Code of Federal Regulations (CFR) as "fraud committed or attempted using the identifying information of another person without permission."[9] Identity theft can both facilitate and be facilitated by other crimes. For example, identity theft may make possible crimes such as bank fraud, document fraud, or immigration fraud, and it may be aided by crimes such as theft in the form of robbery or burglary.[10] Therefore, one of the primary challenges in analyzing the trends in identity theft (e.g., offending, victimization, or prosecution rates)—as well as the policy issues that Congress may wish to consider—arises from this interconnectivity between identity theft and other crimes.

[7] 18 U.S.C. §1028(a)(7).

[8] These felony violations as outlined in 18 U.S.C. §1028A include theft of public money, property, or records; theft, embezzlement, or misapplication by bank officer or employee theft from employee benefit plans; false personation of citizenship; false statements in connection with the acquisition of a firearm; fraud and false statements; mail, bank, and wire fraud; specified nationality and citizenship violations; specified passport and visa violations; obtaining customer information by false pretenses; specified violations the Immigration and Nationality Act relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card and various other immigration offenses; specified violations of the Social Security Act relating to false statements relating to programs under the act; and specified terrorism violations. The basic penalty for identity theft under 18 U.S.C. §1028 ranges from not more than five years imprisonment to not more than 30 years, depending on the circumstances.

[9] According to the CFR definitional section for the Fair Credit Reporting Act (16 C.F.R. §603.2), "[t]he term ''identifying information'' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—(1) 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; (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) Unique electronic identification number, address, or routing code; or (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))."

[10] Graeme R. Newman and Megan M. McNally, "Identity Theft Literature Review," Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and enforcement, Contract #2005-TO-008, January 2005, http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

Theft vs. Fraud

Identity theft and identity fraud are terms that are often used interchangeably. Identity fraud[11] is the umbrella term that refers to a number of crimes involving the use of false identification—though not *necessarily* a means of identification belonging to another person. Identity theft is the specific form of identity fraud that involves using the personally identifiable information of someone else. Both identity fraud and identity theft are crimes often committed in connection with other violations, as mentioned above. Identity theft, however, may involve an added element of victimization, as this form of fraud may directly affect the life of the victim whose identity was stolen in addition to defrauding third parties (such as the government, employers, consumers, financial institutions, and health care and insurance providers, just to name a few). This report, however, maintains a focus on identity theft rather than the broader term of identity fraud.

Knowledge Element

Another definitional issue is one that was recently before the U.S. Supreme Court. The statutory definitions of identity theft and aggravated identity theft indicate that they are crimes when someone "*knowingly* transfers, possesses, or uses, without lawful authority, a means of identification of another person" in conjunction with specified felony violations outlined in the U.S. Code. The definitional element under question was the word "knowingly." In *Flores-Figueroa v. United States*, the Court decided that in order to be found guilty of aggravated identity theft, a defendant must have knowledge that the means of identification he used belonged to another individual.[12] It is not sufficient to only have knowledge that the means of identification used was not his own. Although the case before the Court specifically involved aggravated identity theft, the issue may apply to the identity theft statute as well, due to its overlap in wording about the element of knowledge.

Since the Court has issued its final decision in *Flores-Figueroa v. United States*, Congress may wish to consider whether there is a need to clarify the difference between these two types of knowledge in the U.S. Code. If a clarification is warranted, Congress may wish to consider whether the identity theft and aggravated identity theft statutes should be amended to reflect the definitions of both types of knowledge.

Legislative History[13]

Until 1998, identity theft was not a federal crime.[14] Leading up to Congress designating identity theft as a federal crime, identity fraud was on the rise, and the Internet was increasingly being

[11] Identity fraud became a federal crime through the False Identification Crime Control Act of 1982 (P.L. 97-398), and it is codified at 18 U.S.C. §1028.

[12] *Flores-Figueroa v. United States*, 129 S. Ct. 1186 (2009).

[13] The legislation described in this section covers those Acts directly related to the identity theft statutes. Other statutes, such as the credit reporting statutes, indirectly address identity theft by possibly assisting victims, however, they are not discussed here. For more information on the scope of federal laws relating to identity theft, see archived CRS Report RL31919, *Federal Laws Related to Identity Theft*, by Gina Stevens. See also CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities*, by Margaret Mikyung Lee.

[14] The first state to enact an identity theft law was Arizona in 1996.

used as a method of defrauding innocent victims. Law enforcement and policymakers suggested that the current laws at the time were ineffective at combating the growing prevalence of identity theft;[15] the laws were not keeping up with technology, and stronger laws were needed to investigate and punish identity thieves.[16] In addition, policymakers also suggested that industries that handled records containing individuals' personally identifiable information—such as credit, medical, and criminal records—needed superior methods to ensure the validity of the information they collected and utilized.

Identity Theft Assumption Deterrence Act

In 1998, Congress passed the Identity Theft Assumption Deterrence Act (P.L. 105-318), which criminalized identity theft at the federal level. In addition to making identity theft a crime, this act provided penalties for individuals who either committed or attempted to commit identity theft and provided for forfeiture of property used or intended to be used in the fraud. It also directed the Federal Trade Commission (FTC) to record complaints of identity theft, provide victims with informational materials, and refer complaints to the appropriate consumer reporting and law enforcement agencies. The FTC now records consumer complaint data and reports it in the Identity Theft Data Clearinghouse; identity theft complaint data are available for 2000 and forward.[17]

Identity Theft Penalty Enhancement Act

Congress further strengthened the federal government's ability to prosecute identity theft with the passage of the Identity Theft Penalty Enhancement Act (P.L. 108-275).[18] This act established penalties for *aggravated identity theft*, in which a convicted perpetrator could receive additional penalties (two to five years' imprisonment) for identity theft committed in relation to other federal crimes. Examples of such federal crimes include theft of public property, theft by a bank officer or employee, theft from employee benefit plans, false statements regarding Social Security and Medicare benefits, several fraud and immigration offenses, and specified felony violations pertaining to terrorist acts.

Identity Theft Enforcement and Restitution Act of 2008

Most recently, Congress enhanced the identity theft laws by passing the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 110-326). Among other elements, the act authorized restitution to identity theft victims for their time spent recovering from the harm caused by the actual or intended identity theft.

[15] Before identity theft became a federal crime, identity fraud had been established as a crime in the False Identification Crime Control Act of 1982 (P.L. 97-398). However, the identity fraud statute did not contain a specific theft provision.

[16] From remarks James Bauer, Deputy Assistant Director, Office of Investigations, U.S. Secret Service, before the U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, *The Identity Theft and Assumption Deterrence Act*, 105th Cong., 2nd sess., May 20, 1998.

[17] Unless otherwise noted in this report, all dates refer to calendar years rather than fiscal years.

[18] Aggravated Identity Theft is codified at 18 U.S.C. §1028A.

Identity Theft Task Force

In addition to congressional efforts to combat identity theft, there have been administrative efforts as well. The President's Identity Theft Task Force (Task Force) was established in May 2006 by Executive Order 13402.[19] The task force was created to coordinate federal agencies in their efforts against identity theft, and it was charged with creating a strategic plan to combat (increase awareness of, prevent, detect, and prosecute) identity theft. It was composed of representatives from 17 federal agencies.[20]

Recommendations

In April 2007, the task force authored a strategic plan for combating identity theft in which it made recommendations in four primary areas:

- preventing identity theft by keeping consumer data out of criminals' hands,
- preventing identity theft by making it more difficult for criminals to misuse consumer data,
- assisting victims in detecting and recovering from identity theft, and
- deterring identity theft by increasing the prosecution and punishment of identity thieves.[21]

With respect to identity theft prevention, the task force suggested that decreasing the use of Social Security numbers (SSNs) in the public sector and reviewing the use of SSNs in the private sector could help prevent identity theft. Also, the task force suggested that educating employers and individuals on how to safeguard data, as well as establishing national data protection and breach notification standards, could further aid in preventing identity theft.

Relating to victim assistance, the task force suggested that identity theft victims may be better served if first responders were specially trained to assist this particular class of victim. It also addressed victim redress by recommending that identity theft victims be able to obtain an alternative identification document after the theft of their identities. Through the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 110-326), Congress responded to the task force's recommendation that criminal restitution statutes allow victims to be compensated for their time in recovering from the actual or attempted identity theft.

---

[19] Executive Order 13402, "Strengthening Federal Efforts To Protect Against Identity Theft," 71 *Federal Register* 93, May 15, 2006.

[20] Members of the task force included the Attorney General (chair), the Chairman of the Federal Trade Commission (co-chair), the Secretary of the Treasury, the Secretary of Commerce, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Commissioner of Social Security, the Chairman of the Board of Governors of the Federal Reserve System, the Chairperson of the Board of Directors of the Federal Deposit Insurance Corporation, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Chairman of the National Credit Union Administration Board, the Postmaster General, the Director of the Office of Personnel Management, and the Chairman of the Securities and Exchange Commission.

[21] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007, at http://www.identitytheft.gov/reports/StrategicPlan.pdf.

Regarding identity theft deterrence, the task force recommended enhancing information gathering and sharing between domestic law enforcement agencies and the private sector, ramping up identity theft training for law enforcement and prosecutors, and increasing enforcement and prosecution of identity theft. The task force also promoted international cooperation to decrease identity theft through identifying countries that may be safe havens for identity thieves, encouraging anti-identity theft legislation in other countries, and increasing international cooperation in the investigation and prosecution of identity theft.

Legislative Recommendations

More specifically, the task force recommended that Congress close gaps in the federal criminal statues to more effectively prosecute and punish identity theft-related offenses by

- amending the identity theft and aggravated identity theft statutes so that thieves who misappropriate the identities of corporations and organizations—and not just the identities of individuals—can be prosecuted,
- amending the aggravated identity theft statute by adding new crimes as predicate offenses for aggravated identity theft violations,
- amending the statute criminalizing the theft of electronic data by eliminating provisions requiring that the information be stolen through interstate communications,
- amending the computer fraud statute by eliminating the requirement that damage to a victim's computer exceed $5,000,
- amending the cyber-extortion statute by expanding the definition of cyber-extortion, and
- ensuring that the Sentencing Commission allows for enhanced sentences imposed on identity thieves whose actions affect multiple victims.[22]

Congress has already taken steps to address some of these task force recommendations. Through the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 110-326), Congress, among other things, eliminated provisions in the U.S. Code requiring the illegal conduct to involve interstate or foreign communication, eliminated provisions requiring that damage to a victim's computer amass to $5,000, and expanded the definition of cyber-extortion.

However, Congress has not yet addressed the task force recommendation to expand the identity theft and aggravated identity theft statutes to apply to corporations and organizations as well as to individuals, nor has it addressed the recommendation to expand the list of predicate offenses for aggravated identity theft. Issues surrounding these recommendations are analyzed in the section "Potential Issues for Congress."

[22] Ibid.

Red Flags Rule[23]

The Identity Theft Red Flags Rule, issued in 2007, requires creditors and financial institutions to implement identity theft prevention programs. It is implemented pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003 (P.L. 108-159). The FACT Act amended the Fair Credit Reporting Act (FCRA)[24] by directing the FTC, along with the federal banking agencies and the National Credit Union Administration, to develop Red Flags guidelines. These guidelines require creditors[25] and financial institutions[26] with "covered accounts"[27] to develop and institute written identity theft prevention programs. According to the FTC, the identity theft prevention programs required by the rule must provide for

- identifying patterns, practices, or specific activities—known as "red flags"—that could indicate identity theft and then incorporating those red flags into the identity theft prevention program;
- detecting those red flags that have been incorporated into the identity theft prevention program;
- responding to the detection of red flags; and
- updating the identity theft prevention program periodically to reflect any changes in identity theft risks.[28]

Possible "red flags" could include

- alerts, notifications, or warnings from a consumer reporting agency;

[23] The Red Flags Rule is listed in the Code of Federal Regulations at 16 C.F.R. §681.2. The Red Flags Rule was issued jointly by the FTC; the Office of the Comptroller of the Currency, Treasury; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision, Treasury; and the National Credit Union Administration. The final rules are available in the Federal Register. See Department of the Treasury, Office of the Comptroller of the Currency; Federal Reserve System; Federal Deposit Insurance Corporation; Department of the Treasury, Office of Thrift Supervision; National Credit Union Administration; Federal Trade Commission, "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule," 72 *Federal Register* 63718 - 63775, November 9, 2007.

[24] The FCRA is codified at 15 U.S.C. §1681.

[25] Under the Red Flags Rule, a creditor is defined as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit," 15 U.S.C. §1691a. The Red Flag Program Clarification Act of 2010 (S. 3987), signed by President Obama on December 18, 2010, limits this definition of a creditor, excluding any creditor "that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person."

[26] Under the Red Flags Rule, a financial institution is defined as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in §461(b) of title 12) belonging to a consumer," 15 U.S.C. §1681a(t).

[27] A covered account is one that is used primarily for personal, family, or household purposes, and that involves multiple payments or transactions. These include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, savings accounts, and other accounts for which there is a foreseeable risk of identity theft. The Rule also requires creditors and financial institutions to periodically determine whether they maintain any covered accounts, 72 *Federal Register* 63719.

[28] Federal Trade Commission, "Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy," press release, October 31, 2007, http://ftc.gov/opa/2007/10/redflag.shtm.

- suspicious documents;
- suspicious personally identifiable information, such as a suspicious address;
- unusual use of—or suspicious activity relating to—a covered account; and
- notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.[29]

The deadline for creditors and financial institutions to comply with the Red Flags Rule was originally set at November 1, 2008. However, many of the organizations affected by the Red Flags Rule were not prepared to institute their identity theft prevention programs by this date. Therefore, the FTC moved the deadline to May 1, 2009,[30] further extended the compliance date to November 1, 2009,[31] and later to June 1, 2010.[32] The final enforcement date was set at December 31, 2010,[33] and this last extension was, in part, a result of the debate over whether Congress wrote the FACT Act Red Flags provision too broadly by including all entities qualifying as creditors and financial institutions (discussed further below).

The effect that the Red Flags Rule will have on the prevalence of identity theft remains uncertain. One potential effect is that the Red Flags Rule may help creditors and financial institutions prevent identity theft by identifying potential lapses in security or suspicious activities that could lead to identity theft. This could possibly lead to an overall decrease in the number of identity theft incidents reported to the FTC, as well as the number of identity theft cases investigated and prosecuted. Once detected, the Red Flags Rule requires that the creditor or financial institution respond to the identified red flag. One response option that creditors and financial institutions might include in their prevention programs is to notify consumers or law enforcement of data breaches that could potentially lead to the theft of consumers' personally identifiable information. While notification is not a required element in the identity theft prevention programs,[34] early notification could lead to consumers taking swift action to prevent identity theft or mitigate the severity of the damage that could result if they had not been notified as quickly.

When the Red Flags Rule was created, the FTC originally estimated that it would impact approximately 11.1 million creditors and financial institutions required to implement the identity theft prevention programs.[35] The FTC estimated the total annual labor costs (for each of the first three years the rule is in effect) for all creditors and financial institutions covered by the rule to be

[29] http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

[30] Federal Trade Commission, "FTC Will Grant Six-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs," press release, October 22, 2008, http://www.ftc.gov/opa/2008/10/redflags.shtm.

[31] Federal Trade Commission, "FTC Will Grant Three-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Adopt Identity Theft Prevention Programs," press release, April 30, 2009, http://www.ftc.gov/opa/2009/04/redflagsrule.shtm.

[32] Federal Trade Commission, "FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule," press release, October 30, 2009, http://www.ftc.gov/opa/2009/10/redflags.shtm.

[33] Federal Trade Commission, "FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule," press release, May 28, 2010, http://www.ftc.gov/opa/2010/05/redflags.shtm.

[34] The FTC has published a guide to assist businesses in creating the identity theft prevention programs, available at Federal Trade Commission, *Fighting Fraud With the Red Flags Rule: A How-To Guide for Business*, March 2009, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf.

[35] Identity Theft Red Flags Final Rule, p. 63741.

about $143 million.[36] Some entities considered creditors or financial institutions under the rule expressed concern that the burden of the rule overlaps with burdens already incurred under other regulations. For example, the American Bar Association (ABA) questioned whether lawyers are considered "creditors" under the Red Flags Rule because they generally do not require payment until after services are rendered. Further, the American Medical Association indicated that physicians should be exempt from the Red Flags Rule because of patient privacy and security protections required by the Health Insurance Portability and Accountability Act (HIPAA).[37] In addition, there may have been concern that to avoid being considered creditors, some physicians could possibly require full payment at the time of service (rather than allowing deferred payments). This could in turn lead to some patients avoiding potentially necessary treatment if they are unable to pay in full at the time of service; on the other hand, the rule may have no effect on patients' willingness to seek medical treatment. The Red Flag Program Clarification Act of 2010 (P.L. 111-319), signed by President Obama on December 18, 2010, limits the Red Flags Rule's definition of a creditor, excluding any creditor "that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person." This legislation does not exempt any broad categories of businesses or entities, but the majority of businesses in certain categories—such as physicians—would be exempt from Red Flags Rule compliance. The actual effects of the Red Flags Rule—including effects on identity theft rates as well as any indirect consequences—will not be evident until after full implementation by creditors and financial institutions. Congress may consider monitoring the effects of the impending Red Flags Rule on subsequent identity theft rates.

Trends in Identity Theft

As previously mentioned, research indicates that in 2010, about 8.1 million Americans were victims of identity theft. This is a decrease of about 3 million from the approximately 11.1 million who were victimized in 2009.[38] Consumer complaints of identity theft to the FTC exhibited a corresponding decrease. The FTC received 250,854 consumer complaints of identity theft in 2010, down from 278,356 complaints in 2009. However, identity theft incidents reported to the FTC remain a fraction of the estimated victim population. There is a noted difference between the 250,854 complaints received by the FTC in 2010 and survey data indicating that about 8.1 million people were actually victimized. This disparity between research on identity theft victimization and consumer reports could be a result of several factors. For one, while some identity theft victims may file a report with the FTC, others may file complaints with credit bureaus, while still others may file complaints with law enforcement. Not all victims, however, may file complaints with consumer protection entities, credit reporting agencies, and law enforcement. Another possible factor contributing to the disparity is that victims may not—for any number of reasons—report an identity theft incident. These individuals, however, may be more likely to indicate the incident on a survey prompting them about their experiences with identity theft or fraud.

[36] Ibid. Cost estimates are provided by OMB in three-year increments. Therefore, cost estimates for subsequent years are unavailable and could change from the estimates provided for the first three years.

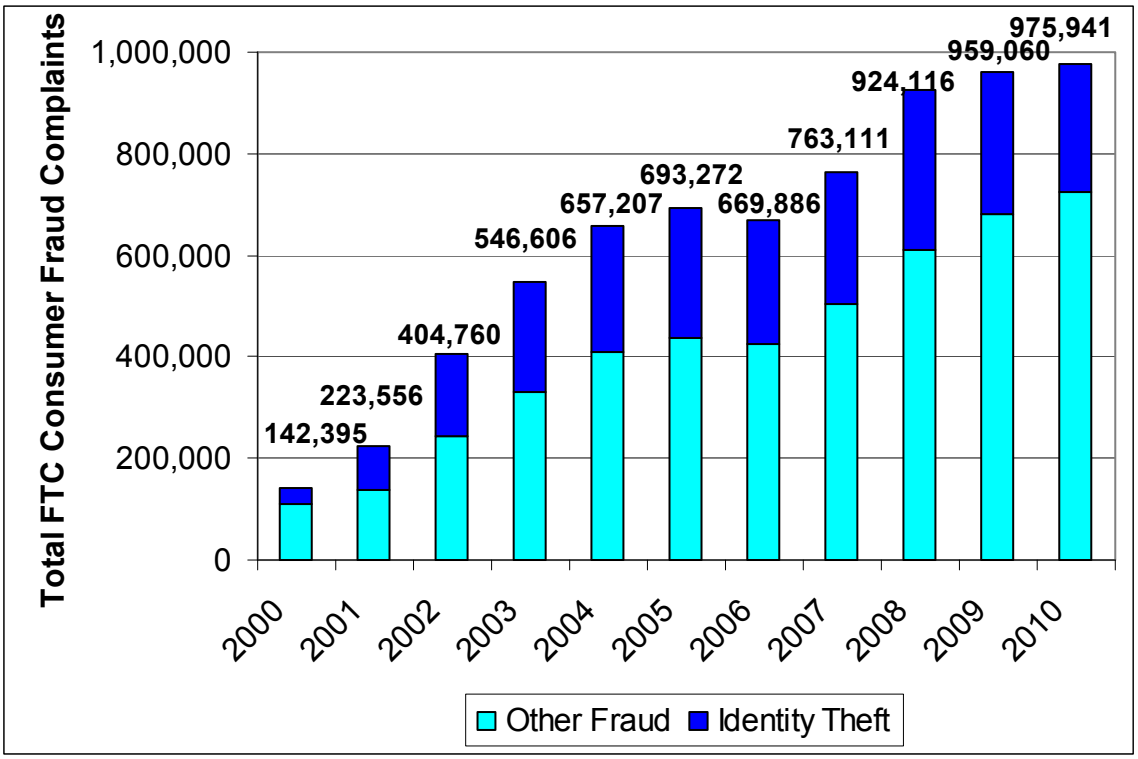
[37] Letter from American Medical Association et al. to William E. Kovacic, Chairman, U.S. Federal Trade Commission, September 30, 2008, http://www.ama-assn.org/ama1/pub/upload/mm/31/ftc_letter20080930.pdf. HIPAA was enacted by P.L. 104-191. Fore more information on HIPAA or health information privacy, see CRS Report R40546, *The Privacy and Security Provisions for Health Information in the American Recovery and Reinvestment Act of 2009*, by Gina Stevens and Edward C. Liu.

[38] Javelin Strategy & Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011.

Since the FTC began recording consumer complaint data in 2000, identity theft has remained the most common consumer fraud complaint. **Figure 1** illustrates the number of identity theft complaints received by the FTC between 2000 and 2010 in relation to the number of all other fraud complaints received. According to CRS analysis, since 2000, the number of identity theft complaints has averaged about 35% of the total number of consumer complaints received by the FTC.[39]

Figure 1. FTC Consumer Complaint Data

Identity Theft and Other Fraud for 2000-2010



Source: CRS presentation of FTC Identity Theft Clearinghouse data. Annual reports for each calendar year are available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

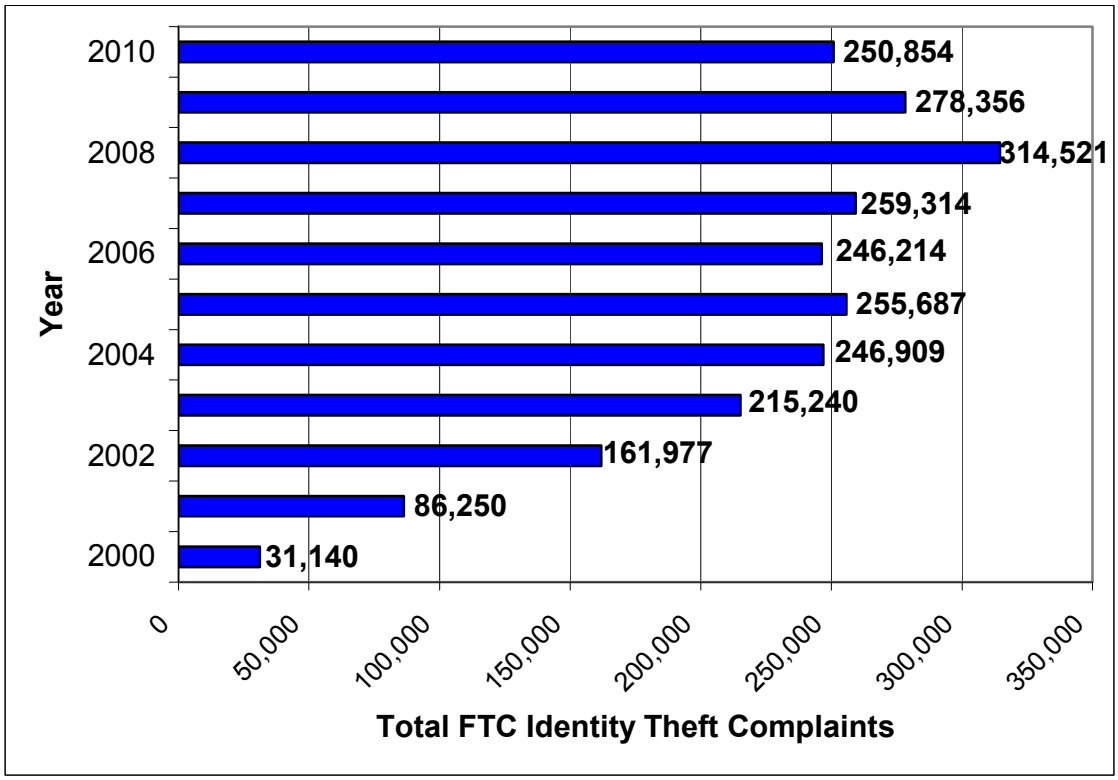
Notes: Data indicate the number of identity theft and other fraud complaints received by the FTC each calendar year. According to CRS analysis, between 2000 and 2010, the number of identity theft complaints has averaged about 35% of the total number of consumer complaints received by the FTC. The percentage has ranged between about 22% and about 40%.

Identity theft has remained the dominant consumer fraud complaint to the FTC. However, while the number of overall identity theft complaints generally increased between 2000 (when the commission began recording identity theft complaints) and 2008, the number of complaints decreased in both 2009 and 2010. **Figure 2** illustrates these trends in identity theft complaints reported to the FTC.

[39] Between 2000 and 2010, the proportion of consumer fraud complaints that are classified as identity theft complaints has ranged from about 22% to about 40%. The total number of identity theft and other fraud complaints reported to the FTC are available from the annual Identity Theft Clearinghouse Data reports available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

Figure 2. FTC Identity Theft Complaint Data

2000-2010



Source: CRS presentation of FTC Identity Theft Clearinghouse data. Annual reports for each calendar year are available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdfl.

Notes: Data indicate the number of identity theft complaints received by the FTC each calendar year.

Perpetrators

Increasing globalization and the expansion of the Internet have provided a challenging environment for law enforcement to both identify and apprehend identity thieves targeting persons residing in the United States. For one, these criminals may be operating from within U.S. borders as well as from beyond. There is no publically available information, however, delineating the proportion of identity theft (or other crimes known to be identity theft-related) committed by domestic and international criminals.[40] Secondly, while some identity thieves operate alone, others operate as part of larger criminal networks or organized crime syndicates. The FBI has indicated that it, for one, targets identity theft investigations on larger criminal networks.[41] These criminal networks may involve identity thieves located in various cities across the United States or in multiple cities around the world, and these criminals may be victimizing not only Americans, but persons living in countries across the globe. In a joint study by Verizon

[40] Statistics are available on the proportion of cyber-related crimes committed by perpetrators from various countries. However, only a proportion of those crimes are identity theft crimes, and analysts therefore cannot reliably extrapolate the proportion of identity theft crimes committed by domestic and international criminals.

[41] Federal Bureau of Investigation, *Financial Crimes Report to the Public*, Fiscal Year 2006, http://www.fbi.gov/publications/financial/fcs_report2006/publicrpt06.pdf.

and the U.S. Secret Service of selected data breaches of businesses around the globe during 2010, 58% of data breaches by "external agents"—sources outside the compromised organization—were attributed to organized crime.[42] It is unknown, however, how many of these records compromised by organized crime were used in identity theft and related crimes. A third challenge in identifying identity thieves is that perpetrators may operate under multiple identities including actual identities, various stolen identities, and cyber identities and nicknames.

Investigations and Prosecutions

As mentioned earlier, identity theft is defined broadly, and it is directly involved in a number of other crimes and frauds. As a result, there are practical investigative implications that influence analysts' abilities to understand the true extent of identity theft in the United States. For instance, only a proportion (the exact number of which is unknown) of identity theft incidents are reported to law enforcement. While some instances may be reported to consumer protection agencies (e.g., the FTC), credit reporting agencies (e.g., Equifax, Experian, and Trans Union), and law enforcement agencies, some instances may be reported to only one. For example, the FTC indicates that of the 42% of identity theft complaints that included information on whether the theft was reported to law enforcement, 72% were reported to law enforcement.[43]

Another issue that may affect analysts' abilities to evaluate the true extent of identity theft is that law enforcement agencies may not uniformly report identity theft because crime incident reporting forms may not necessarily contain specific categories for identity theft. In addition, there may not be standard procedures for recording the identity theft component of the criminal violations of primary concern.[44] Issues such as these may lead to discrepancies between data available on identity theft reported by consumers, identity theft reported by state and local law enforcement, and identity theft investigated and prosecuted by federal law enforcement.

Various federal agencies are involved in investigating identity theft, including the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the United States Postal Inspection Service (USPIS), the Social Security Administration Office of the Inspector General (SSA OIG), and the U.S. Immigration and Customs Enforcement (ICE). In addition, federal law enforcement agencies may work on task forces with state and local law enforcement as well as with international authorities to bring identity thieves to justice. The Department of Justice (DOJ) is responsible for prosecuting federal identity theft cases.

[42] Wade Baker et al., 2011 Data Breach Investigations Report: A Study Conducted by the Verizon RISK Team in Cooperation with the United States Secret Service and the Dutch High Tech Crime Unit, Verizon, 2011, pp. 17-20, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf. Of note, external agents were involved in 92% of all data breaches.

[43] Federal Trade Commission, *Consumer Sentinel Network Data Book for January – December, 2010*, March, 2011, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

[44] Graeme R. Newman and Megan M. McNally, "Identity Theft Literature Review," Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and enforcement, Contract #2005-TO-008, January 2005, http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

Federal Bureau of Investigation (FBI)

The FBI investigates identity theft primarily through its Financial Crimes Section. However, because the nature of identity theft is cross-cutting and may facilitate many other crimes, identity theft is investigated in other sections of the FBI as well. The FBI is involved in over 20 identity theft task forces and working groups around the country. It is also involved in over 80 other financial crimes task forces, which may also investigate cases with identity theft elements.[45] The FBI focuses its identity theft crime fighting resources on those cases involving organized groups of identity thieves and criminal enterprises that affect a large number of victims.[46] The FBI partners with the National White Collar Crime Center (NW3C) to form the Internet Crime Complaint Center (IC3). The IC3 serves the broad law enforcement community to receive, develop, and refer Internet crime complaints—including those of identity theft.[47] In 2010, 9.8% of all Internet crime complaints received by the IC3 were that of identity theft.[48] However, other complaint categories such as credit card fraud may have involved incidents of identity theft as well.

United States Secret Service (USSS)

The USSS serves a dual mission of (1) protecting the nation's financial infrastructure and payment systems to safeguard the economy and (2) protecting national leaders.[49] In carrying out the former part of this mission, the USSS conducts criminal investigations into counterfeiting, financial crimes, computer fraud, and computer-based attacks on the nation's financial and critical infrastructures. The Secret Service has 38 Financial Crimes Task Forces and 31 Electronic Fraud Task Forces that investigate identity theft, as well as a number of other crimes.[50] In FY2010, the Secret Service arrested 4,040 suspects for crimes related to identity theft, and in FY2011, they arrested 4,570 such suspects.[51]

United States Postal Inspection Service (USPIS)

The USPIS is involved in inter-agency task forces investigating identity theft and is the lead federal investigative agency when identity thieves have used the postal system in conducting their fraudulent activities. The most recent USPIS data indicate that in FY2010, the USPIS participated in 18 identity theft task forces, and postal inspectors arrested 759 identity theft suspects—from

[45] U.S. Department of Justice, *Fact Sheet: The Work of the President's Identity Theft Task Force*, September 19, 2006, p. 3, http://www.ftc.gov/os/2006/09/060919IDtheftfactsheet.pdf.

[46] Federal Bureau of Investigation, *Financial Crimes Report to the Public*, Fiscal Year 2006, http://www.fbi.gov/publications/financial/fcs_report2006/publicrpt06.pdf.

[47] See the IC3 website at http://www.ic3.gov/default.aspx. Among the many Internet crimes reported to the IC3 are identity theft and phishing. Phishing refers to gathering identity information from victims under false pretences, such as pretending to be a representative of a financial institution collecting personal information to update financial records.

[48] The IC3 received a total of 303,809 Internet crime complaints. However, it did not make publically available the exact number of these complaints which were identity theft complaints, but rather indicated that identity theft made up about 9.8% of total Internet crime complaints. Internet Crime Complaint Center, *2010 Internet Crime Report*, http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

[49] 18 U.S.C. §3056.

[50] U.S. Secret Service, *United States Secret Service, Fiscal Year 2010 Annual Report*, http://www.secretservice.gov/USSS2010AYweb.pdf.

[51] Information provided to CRS by the USSS office of Congressional Affairs.

both USPIS investigations and task force investigations in which the USPIS was involved.[52] In addition to investigating identity theft, the USPIS has been involved in delivering educational presentations to consumer groups to assist in preventing identity theft, and inspectors are involved in sponsoring outreach programs for victims of identity theft; in FY2010, they provided 667 cases of identity theft victim assistance.[53] Examples of victim services include notifying victims of potential identity theft if the USPIS discovers compromised identities as well as assisting in victim restitution by providing victims money from the funds forfeited as a result of USPIS identity theft investigations.[54]

Social Security Administration Office of the Inspector General (SSA OIG)

Because the theft and misuse of Social Security numbers (SSNs) is one of the primary modes of identity theft, the SSA OIG is involved in investigating identity theft. The SSA has programs to assist victims of identity theft who have had their SSNs stolen or misused by placing fraud alerts on their credit files, replacing Social Security cards, issuing new Social Security numbers in specific instances, and helping to correct victims' earnings records.[55] The SSA OIG protects the integrity of the SSN by investigating and detecting fraud, waste, and abuse. It also determines how the use or misuse of SSNs influences programs administered by the SSA. The SSA OIG is involved in providing a limited range of SSN verification for law enforcement agencies. Further, the SSA OIG maintains a hotline for consumers to report identity theft, and then this data is transferred to the FTC to be included in their consumer complaint database.[56]

Immigration and Customs Enforcement

The U.S. Immigration and Customs Enforcement (ICE) investigates cases involving identity theft, particularly immigration cases that involve document and benefit fraud. In FY2008, ICE conducted 3,636 investigations of document and benefit fraud. In addition, it made 1,652 criminal arrests and seized about $10.3 million related to document and benefit fraud.[57] In 2006, ICE created Document and Benefit Fraud Task Forces (DBFTFs). These DBFTFs, located in 18 cities throughout the United States, are aimed at dismantling and seizing the financial assets of criminal organizations that threaten the nation's security by engaging in document and benefits fraud.

Department of Justice

The U.S. Attorneys Offices (USAOs) prosecute federal identity theft cases referred by the various investigative agencies. CRS was unable to determine the proportion of identity theft cases

[52] Data provided to CRS by the USPIS Office of Congressional Affairs, November 30, 2011.

[53] U.S. Postal Inspection Service, *U.S. Postal Inspection Service Annual Report FY2010*, http://www.postalinspectorsvideo.com/uspis/AnnualReport2010.pdf.

[54] United States Postal Inspection Service, *FY2007 Annual Report of Investigations of the United States Postal Inspection Service*, January 2008, pp. 16-17, https://postalinspectors.uspis.gov/radDocs/pubs/AR2007.pdf.

[55] Social Security Administration, *Identity Theft Fact Sheet*, October 2006, http://www.socialsecurity.gov/pubs/idtheft.htm.

[56] Information provided to CRS by the Social Security Administration, Office of the Inspector General, Office of Congressional Affairs, March 25, 2009.

[57] U.S. Immigration and Customs Enforcement, *ICE Fiscal Year 2008 Annual Report: Protecting National Security and Upholding Public Safety*, 2008, p. iv, http://www.ice.gov/doclib/pi/reports/ice_annual_report/pdf/ice08ar_final.pdf.

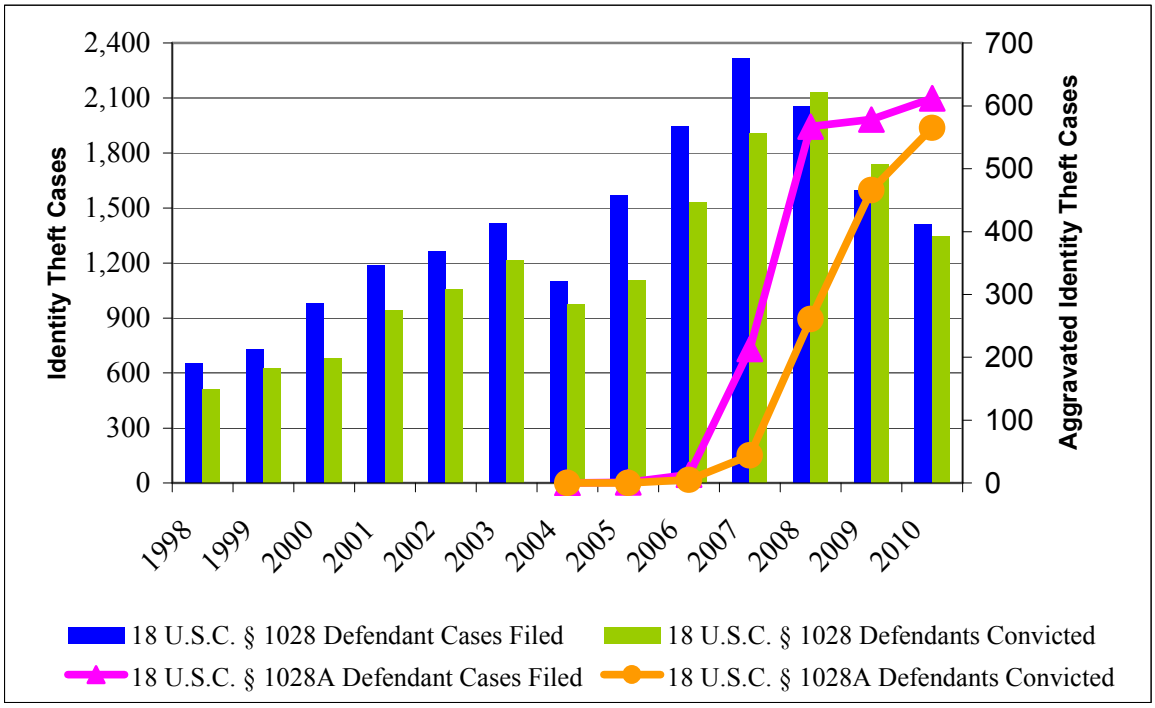
referred to the USAOs by each investigative agency for several reasons. For one, some of the investigations reported by each agency are investigations conducted by a task force, to which several agencies may have contributed. Consequently, these investigations may be reported by each participating agency. If the total number of reported investigations from each agency were combined, it is likely that the overall number of identity theft investigations would be inflated because of double (or more) reporting of an investigation from multiple agencies. A second factor is that the USAOs do not track the proportion of case referrals by statute; rather, they track case referrals by program area. For instance, the proportion of identity theft (18 U.S.C. §1028) and aggravated identity theft (18 U.S.C. §1028A) case referrals from each agency are not tracked according to the charging statutes. Identity theft cases fall under several programmatic categories—including white collar crime and immigration—which also contain several other crimes. Thus, trends in federal identity theft and aggravated identity theft cases may be better tracked by the number of total cases referred to and prosecuted by the USAOs, irrespective of the referring agency.

Somewhat mirroring the trend in identity theft complaints reported to the FTC, there was a recent decrease in the number of identity theft cases prosecuted by DOJ. **Figure 3** illustrates the number of identity theft (18 U.S.C. §1028) and aggravated identity theft (18 U.S.C. §1028A) cases filed (specifically, the number of *defendant* cases filed[58]) with the USAOs as well as defendants convicted between FY1998 and FY2010.

[58] There may be multiple defendants in a case. Of note, **Figure 3** depicts the number of defendants (rather than the number of cases) prosecuted and convicted on charges of identity theft and aggravated identity theft for FY1998 through FY2010.

Figure 3. Federal Identity Theft and Aggravated Identity Theft Cases

Defendant Cases Filed and Defendants Convicted FY1998-FY2010



Source: CRS analysis of data provided by the USAO, Congressional Affairs.

Notes: Identity theft defendant cases filed and convictions are plotted on the left Y-axis while the aggravated identity theft cases filed and convictions are plotted on the right Y-axis. Identity theft is prosecuted under 18 U.S.C. §1028 and aggravated identity theft is prosecuted under 18 U.S.C. §1028A. Identity theft became a federal crime in 1998, and aggravated identity theft became a federal crime in 2004. Data include all cases filed with the USAOs containing an identity theft or aggravated identity theft violation, and are not limited to those cases where identity theft or aggravated identity theft is the lead charge. This includes data filed with the USAOs from all federal agencies.

While the number of identity theft cases filed and the number of defendants convicted both decreased in FY2009 and FY2010 relative to FY2008, the numbers of aggravated identity theft cases filed and defendants convicted have continued to increase. Still, if the identity theft and aggravated identity theft data are combined, total case filings and prosecutions both decreased in FY2009 and FY2010. There are several possible explanations for these trends. One possibility is that there has been a decrease in the overall number of identity theft incidents, and law enforcement has been responding proportionally by arresting fewer identity thieves and filing fewer cases with the U.S. Attorneys' Offices. While the decrease in the number of identity theft complaints to the FTC, as reflected in **Figure 2**, suggests that this may be a viable explanation, some research indicates that the number of individuals victimized by identity thieves is actually continuing to increase.[59] A second possibility is that there has actually been an increase in the number of identity theft incidents, but that either these criminals are evading federal law enforcement or law enforcement has dedicated fewer resources toward combating identity theft,

[59] Javelin Strategy & Research, "Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back," press release, February 10, 2010, https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail.

which has resulted in decreased investigations and prosecutions. Yet another explanation may be that fewer perpetrators are actually impacting a greater number of victims. As criminals become more technologically savvy, they may be able to expand their reach to a greater number of victims.

As illustrated in **Figure 3**, the number of identity theft cases filed in FY2010 maintained the downward trend from FY2008 and FY2009. This was accompanied by a sustained increase in aggravated identity theft case filings. Several factors could possibly contribute to these divergent trends. One explanation is that some cases in which defendants would have been charged with identity theft in earlier years may more recently have resulted in defendants being charged with aggravated identity theft. Therefore, a decrease in identity theft case filings may be complemented with an increase in aggravated identity theft case filings. As mentioned before, aggravated identity theft became a federal crime in 2004, and is reflected in **Figure 3** by the increase in aggravated identity theft case filings and convictions in later years. Analysts would need to evaluate several more years of data to make any reliable or valid predictions regarding factors contributing to fluctuations in identity theft and aggravated identity theft prosecutions.

Domestic Impact

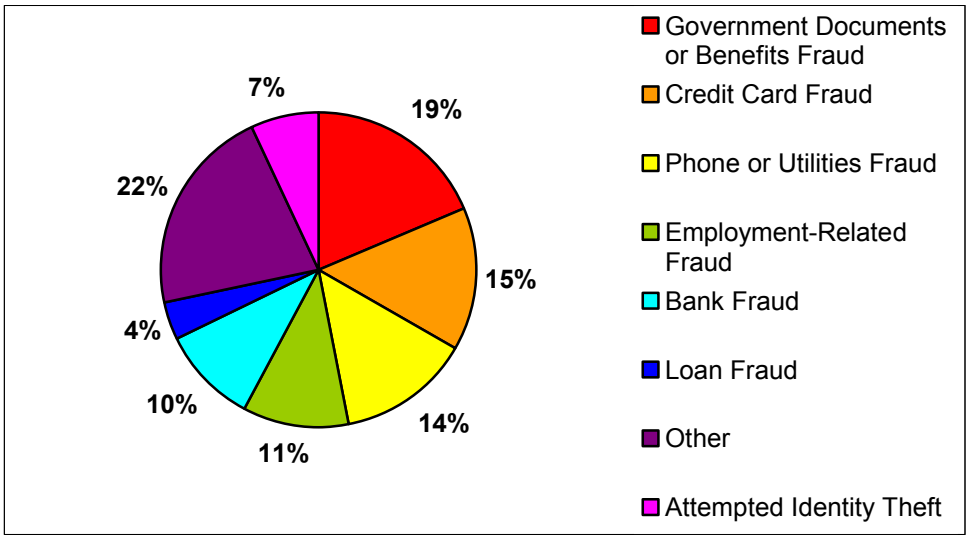
As mentioned, in 2010, about 8.1 million Americans were reportedly victims of identity fraud.[60] And these are the known cases. The Federal Trade Commission (FTC) recognizes two primary forms of identity theft: existing account fraud and new account fraud. Existing account fraud refers to the misuse of a consumer's existing credit card, debit card, or other account, while new account fraud refers to the use of stolen consumer identifying information to open new accounts in the consumer's name.[61] **Figure 4** illustrates the most common misuses of victims' identities.

[60] Javelin Strategy & Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011.

[61] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Subcommittee on Crime, Terrorism, and Homeland Security, House Committee on the Judiciary, on Protecting Consumer Privacy and Combating Identity Theft*, Washington, DC, December 18, 2007, p. 2, http://www.ftc.gov/os/testimony/P065404idtheft.pdf.

Figure 4. FTC Identity Theft Complaints, 2010

How Victims' Information is Misused



Source: FTC Identity Theft Clearinghouse data, *Consumer Sentinel Network Data Book for January - December 2010*, March 2011, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

Notes: Of the 250,854 identity theft complaints received by the FTC in 2010, the most prevalent form of identity theft was government documents or benefits fraud. About 12% of the identity theft complaints received by the FTC involved more than one form of identity theft. For this reason, the sum of the various types of identity theft included in the figure amounts to greater than 100%. Also, within in the category "other," are complaints of victims' identities being misused across subcategories including evading the law, medical, Internet/e-mail, apartment/house rented, insurance, securities/other investments, property rental fraud, magazines, child support, bankruptcy, miscellaneous, and uncertain. The uncertain subcategory alone accounts for about 9% of all identity theft complaints.

Between 2000—when the FTC began tracking identity theft complaints—and 2008, the FTC consistently reported that the most common misuse of a victim's identity was credit card fraud.[62] In 2008, government documents and benefits fraud became the second most prevalent misuse of a victim's identity, and in 2010, it became the most prevalent.[63] Within the documents/benefits fraud category, the FTC has reported a particularly large increase in identity theft related to tax return fraud. And, tax return-related fraud was involved in about 15.5% of the identity theft complaints received by the FTC in 2010.[64]

Identity theft and the various crimes it facilitates affect the economy and national security of the United States. Selected crimes facilitated by identity theft are outlined in the section below.

[62] Although there are estimates regarding the cost of identity theft to consumers, CRS was unable to locate any comprehensive, reliable data on the costs of identity theft (separate from the total cost of financial fraud) to the credit card industry.

[63] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December, 2010*, March, 2011, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

[64] Ibid.

Credit Card Fraud[65]

After a victim's identity is stolen, the primary criminal use of this information is credit card fraud. Beyond amassing charges on a victim's credit card, identity thieves may sometimes change the billing address so that the victim will not receive the bills and see the fraudulent charges, allowing the thief more time to abuse the victim's identity and credit. If a victim does not receive the bill, and therefore does not pay it, this could aversely affect the victim's credit. In addition to abusing existing credit card accounts, a thief could also open new accounts in the victim's name, incurring more charges on the victim's line of credit. These actions could in turn affect not only the victim's immediate pocketbook, but future credit as well. The Identity Theft Resource Center (ITRC) has predicted that organized crime groups will become more involved in identity theft-related crime such as credit card fraud and that these crimes will become increasingly transnational.[66] As mentioned, criminals are no longer constrained by physical borders, and they can victimize U.S. persons and businesses both from within the United States and from beyond.

- In February 2011, Operation Power Outage led to the arrest of 83 individuals associated with Armenian Power, an Armenian and Eastern European transnational criminal organization. These individuals were allegedly involved in a range of criminal activities including credit card fraud. One scheme is reported to have used skimming devices, secretly installed on cash register machines, to steal customer account information. This information was subsequently used to create counterfeit credit and debit cards.[67]

Document Fraud[68]

Identity thieves can use personally identifiable information to create fake or counterfeit documents such as birth certificates, licenses, and Social Security cards. One way that thieves can use the stolen information is to obtain government benefits in a victim's name. This directly affects the victim if the victim attempts to legitimately apply for benefits and then is denied because someone else may already be (fraudulently) receiving those benefits under the victim's name. The creation of fraudulent documents may, among other things, provide fake identities for unauthorized immigrants[69] living in the United States or fake passports for people trying to illegally enter the United States. In addition, DOJ has indicated that identity theft is implicated in international terrorism. In May 2002, former Attorney General John Ashcroft stated that

> [I]dentity theft is a major facilitator of international terrorism. Terrorists have used stolen identities in connection with planned terrorist attacks. An Algerian national facing U.S. charges of identity theft, for example, allegedly stole the identities of 21 members of a health

[65] Credit card fraud is codified at 18 U.S.C. §1029.

[66] Identity Theft Resource Center, *ITRC Forecasts Black Ice Ahead in 2011*, December 15, 2010, http://www.idtheftcenter.org/artman2/publish/m_press/ITRC_Forecasts_for_2011.shtml.

[67] Federal Bureau of Investigation, *Operation Power Outage: Armenian Organized Crime Group Targeted*, April 3, 2011, http://www.fbi.gov/news/stories/2011/march/armenian_030311/armenian_030311.

[68] Document fraud is codified at 18 U.S.C. §1028. The statutory definition of identity theft is found within this section of the Code at 18 U.S.C. §1028(a)(7).

[69] A complete discussion of immigration-related document fraud is outside the scope of this report, but more information can be found in CRS Report RL34007, *Immigration Fraud: Policies, Investigations, and Issues*, by Ruth Ellen Wasem.

club in Cambridge, Massachusetts, and transferred the identities to one of the individuals convicted in the failed 1999 plot to bomb the Los Angeles International Airport.[70]

Identity theft and resulting document fraud can thus have not only an economic impact on the United States, but a national security impact as well.

- In November 2011, at least 25 individuals were indicted for their alleged roles in large-scale fraudulent document manufacturing rings. Individuals produced fraudulent documents such as Legal Permanent Resident cards, Social Security cards, Mexican Consular Identification cards, and driver's licenses. These fraudulent documents reportedly supported a variety of criminal activities such as credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion schemes.[71]

Employment Fraud

Identity theft can facilitate employment fraud if the thief uses the victim's personally identifiable information to obtain a job. With the currently elevated level of unemployment,[72] policymakers may wish to monitor trends in employment fraud. This form of fraud could aversely affect a victim's credit, ability to file his or her taxes, and ability to obtain future employment, among other things. Not only can identity theft lead to employment fraud, but employment fraud may be a means to steal someone's identity. Identity thieves may use scams that falsely advertise employment as a means to phish for personally identifiable information. The thief can then use this information to commit other crimes while the job-seeking individual remains unemployed and victimized.

Data Breaches and Identity Theft

As mentioned, the number of identity theft complaints reported to the FTC generally increased through 2008 and then declined in 2009 and 2010. The number of reported data breaches followed a similar trend, despite a divergence in 2010. The Identity Theft Resource Center (ITRC) tracks data breaches across the nation, and the resulting statistics indicate that the total number of reported data breaches generally increased between 2005 and 2010, with the only decline in 2009.[73] **Figure 5** illustrates this trend. The IRTC indicates that the number of data

[70] Department of Justice, *Transcript of Attorney General Remarks at Identity Theft Press Conference Held With FTC Trade Commission Chairman Timothy J. Muris and Senator Diane Feinstein*, DOJ Conference Center, May 2, 2002, http://www.usdoj.gov/archive/ag/speeches/2002/050202agidtheftranscript.htm. Also cited in U.S. General Accounting Office, *Identity Fraud: Prevalence and Links to Alien Illegal Activities*, GAO-02-830T, June 25, 2002, p. 9, http://www.gao.gov/new.items/d02830t.pdf.

[71] Federal Bureau of Investigation, "More Than Two Dozen Identified in Massive Fraudulent Document Manufacturing Operation in Los Angeles," press release, November 3, 2011, http://www.fbi.gov/losangeles/press-releases/2011/more-than-two-dozen-identified-in-massive-fraudulent-document-manufacturing-operation-in-los-angeles.

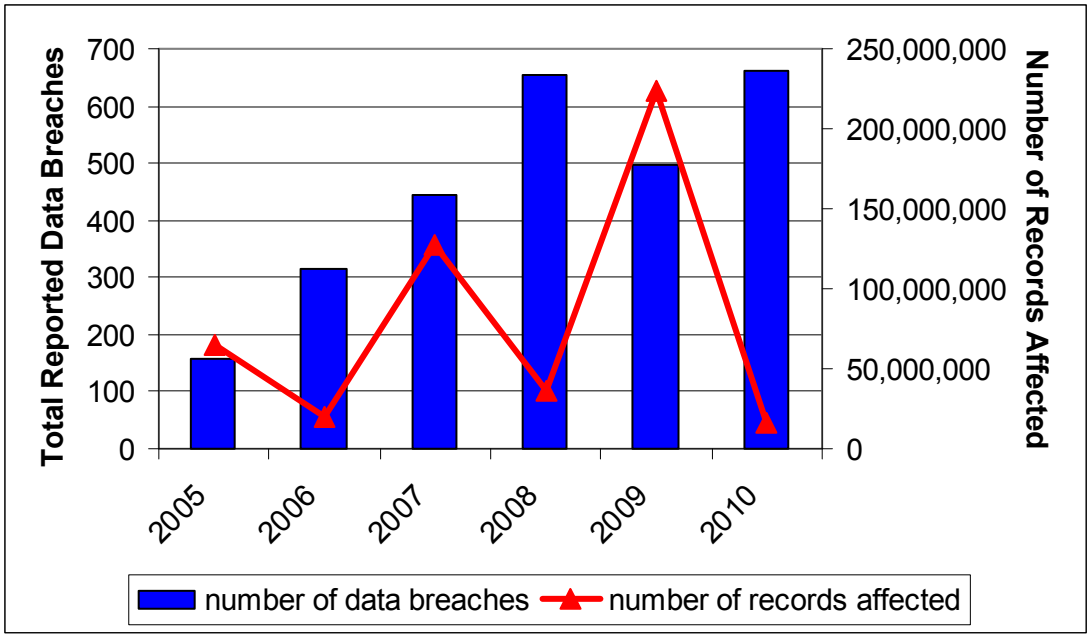
[72] According to the Bureau of Labor Statistics (BLS), the unemployment rate has remained at or above 9.0% since May 2009, http://data.bls.gov/timeseries/LNS14000000.

[73] Identity Theft Resource Center, *2010 Breach Stats*, December 29, 2010, http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202010.pdf. The IRTC indicates that the criteria for qualifying as a data breach is "[a]ny name or number that may be used, alone or in conjunction with other information, to identify a specific individual, including: name, Social Security number, date of birth. Banking or financial account number, credit card or debit card number with or without a PIN, official state or government issued driver's license or identification number, (continued...)

breaches increased from 158 in 2005 to 662 in 2010. Breaches are recorded across five industries: banking/credit/financial, business, education, government/military, and medical/healthcare. In 2010, the business industry experienced the greatest number of data breaches (42.1%), followed by healthcare (24.2%) and government/military (15.7%).

Figure 5. Total Number of Reported Data Breaches and Records Affected

2005-2010



Source: CRS analysis of data provided by the Identity Theft Resource Center, available at http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#.

Notes: Breaches are recorded across five primary industries: banking/credit/financial, business, educational, government/military, and medical/healthcare.

Several factors may influence the number of reported breaches. One such factor may be the increasing number of states that have enacted laws requiring data breach notification.[74] California was the first state to enact such legislation in 2002. As of October 2010, 46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws.[75] The increasing prevalence of state laws requiring breach notification could lead to an increase in reported breaches to law enforcement, media, or the individuals affected. This could lead to an increase in the reported number of data breaches captured by the ITRC. Nonetheless, the actual number of data breaches remains underreported, and the number of breaches does not reflect the

(...continued)

passport identification number, alien registration number, employer or taxpayer identification number, or insurance policy or subscriber numbers; unique biometric data; [or] electronic identification number, address or routing code or telecommunication identifying information or device."

[74] For more information on data breach notification laws affecting the private and public sectors, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

[75] National Conference of State Legislatures, *State Security Breach Notification Laws*, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

magnitude of data breaches. Because of these factors, analysts are unable to say with certainty whether the increase in the number of reported data breaches in 2010 is an accurate reflection of the trend in data breaches.

Furthermore, the number of records affected by each data breach is variable, and in many cases unknown. In 2010, for example, at least 16,167,542 records were put at risk, but information on the exact number of records exposed was only available for 338 (about 51%) of the 662 reported data breaches.[76]

Because available data on known data breaches and reported identity theft incidents are not comprehensive, and because year-to-year changes in one measure may not trend with changes in the other, it can be difficult to determine whether there is a relationship between the two. Intuitively, the data breaches and identity theft may seem to correlate, but some analysts have found that the link may not be very strong. There are several ways to analyze the relationship between data breaches and identity theft. One is to examine the set of data breach victims and determine the proportion of those victims that are also victims of identity theft. Some claim that data breaches are a direct cause of identity theft and may rely on this position to advocate the need for increased data security and data breach notification laws to protect consumers and help with quickly mitigating any potential damage from such data breaches. Meanwhile, other experts claim that less than 1% of data breach victims are also victims of identity theft.[77] Some may use this data to argue against the need for increased data security and breach notification laws, suggesting that such laws could produce a larger cost for businesses than prevention for consumers. In 2010, 7% of U.S. consumers received notification of a data breach. And, Javelin Strategy and Research data suggest that individuals receiving breach notifications "had more than four times higher risk of identity fraud than did those who didn't receive these types of notifications."[78]

Another means to evaluate the relationship between data breaches and identity theft is to examine identity theft victims and analyze the proportion of those victims whose identity was stolen as a result of a data breach. Javelin Strategy and Research (2009) found that about 11% of victims' identities that were stolen had been under the control of a company and were stolen from the company through methods such as data breaches. Most victims (65%) did not know how their identities had been stolen, and some proportion of these could have occurred as a result of a data breach.[79] Synovate (2007) conducted a similar study on behalf of the Federal Trade Commission and found that about 12% of victims' stolen identities had been under the control of a company and were thus accessed via a data breach.[80] The Center for Identity Management and Information Protection at Utica College (2007) evaluated identity theft cases handled by the U.S. Secret

[76] CRS calculated this figure from the data provided from the Identity Theft Resource Center, *2010 Breach Stats*, December 29, 2010, http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202010.pdf.

[77] Findings from Javelin Strategy & Research cited in Ben Worthen, "Cardholders Buy Peace of Mind, If Not Security," *The Wall Street Journal*, March 10, 2009, p. D1.

[78] Javelin Strategy & Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011.

[79] Rachel Kim, *2009 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February 2009, http://www.javelinstrategy.com.

[80] Synovate, *Federal Trade Commission: 2006 Identity Theft Survey Report*, November 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Service between 2002 and 2006 and found that in nearly 27% of the cases, a breach of company-controlled data was the source of the identity theft.[81]

It appears that the stronger relationship between identity theft and data breaches is found when analyzing identity theft victims whose data was obtained through a data breach rather than in analyzing data breaches that result in identity theft. In efforts to curb identity theft, policymakers are left with the issue of how to target data breaches. The question is whether the federal government's role in curbing identity theft should be more preventative, more responsive, or both. One policy option may be for Congress to increase data security for the purpose of preventing those data breaches that could potentially result in identity theft. Congress has already enacted data breach laws targeting certain components of the public and private sectors, such as the Veterans Administration and healthcare providers.[82] Another option could be for Congress to dedicate resources to assisting victims of identity theft and providing sufficient deterrence and punishment measures (in the form of penalties or sanctions). These options are analyzed further below.

Potential Issues for Congress

As Congress debates means to prevent identity theft, mitigate the potential effects of identity theft, and investigate and prosecute identity thieves, there are several issues policymakers may wish to consider. One issue surrounds the extent to which reducing the availability of SSNs may reduce the prevalence of identity theft. A second issue involves the degree to which increasing breach notification requirements may reduce both identity theft and the monetary burden incurred by victims. Yet another issue concerns the adequacy of (1) the current legal definitions of identity theft and aggravated identity theft and (2) the list of predicate offenses for aggravated identity theft.

Identity Theft Prevention

Policymakers may question what the extent of the federal government's role should be in preventing identity theft. One element of this discussion centers around the fact that identity theft is often committed to facilitate other crimes and frauds (e.g., credit card fraud, document fraud, and employment fraud). Consequently, preventing identity theft could proactively prevent other crimes. When policymakers consider the federal government's role in preventing identity theft, they necessarily consider the government's role in preventing interrelated crimes.

[81] Gary R. Gordon, Donald J. Rebovich, and Kyung-Seok Choo, et al., *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, Center for Identity Management and Information Protection, Utica College, OJP, BJA Grant No. 2006-DD-BX-K086, October 2007, http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

[82] For example, the Veterans Affairs Information Security Act, Title IX of P.L. 109-461 requires the Veterans Administration (VA) to implement an information security program to protect its sensitive personal information. For more information, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens. Also, the Health Information Technology for Economic and Clinical Health (HITECH) Act, in P.L. 111-5, established—among other things—a notification requirement for a breach of non-encrypted health information. For further information on the HITECH Act, see CRS Report R40161, *The Health Information Technology for Economic and Clinical Health (HITECH) Act*, by C. Stephen Redhead.

Congress may also consider the various means available to prevent identity theft and evaluate the federal government's role—if any—in implementing them. Possible ways to prevent identity theft include securing data in the private sector, securing data in the public sector, and improving consumer authentication processes.[83]

Securing Social Security Numbers

The prevalence of personally identifiable information—and in particular, of Social Security numbers (SSN)—has been an issue concerning policymakers, analysts, and data security experts.[84] There are few restrictions on the use of SSNs in the private sector, and therefore the use of SSNs is widespread.[85] Some industries, such as the financial services industry, have stricter requirements for safeguarding personally identifying information. There are greater restrictions on the use of SSNs in the public sector, as Congress has already taken direct steps in reducing the prevalence of SSNs in this arena. For example, in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress prohibited states from displaying or electronically including SSNs on driver's licenses, motor vehicle registrations, or personal identification cards. One document that continues to display SSNs, however, is the Medicare identification card. Congress may consider whether the continued display of SSNs on Medicare cards places individuals at undue risk for identity theft as well as for becoming a victim of other crimes facilitated by identity theft and whether it should enact legislation to prohibit the display of SSNs on Medicare cards. Proponents of legislation to remove SSNs from Medicare cards cite reports that as of 2007, 42 million Medicare cards displayed Social Security numbers, potentially placing these individuals at risk for identity theft.[86] Opponents of such legislation may cite that transitioning to a different Medicare identifier has been estimated to cost more than $300 million.[87]

Another policy option to safeguard personally identifiable information that Congress may consider is increasing restrictions on the disclosure of certain forms of personally identifiable information, such as SSNs, in connection with federally funded grant programs. One example of Congress taking such action is in the Violence Against Women and Department of Justice Reauthorization Act of 2005 (P.L. 109-162). Provisions in this act prohibit grantees that receive funds under the Violence Against Women Act of 1994 from disclosing certain personally identifiable information—including SSNs—collected in connection with services through the grant program.[88] Congress may consider whether existing SSN restrictions for federal grant recipients are sufficient or whether the federal government should play a larger role in limiting the use of SSNs—and more specifically, whether it should set limitations as part of eligibility requirements for federal assistance.

---

[83] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007, http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[84] For a complete discussion of the collection, disclosure, and confidentiality of Social Security numbers, see CRS Report RL30318, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*, by Kathleen S. Swendiman.

[85] U.S. Government Accountability Office, *Social Security Numbers: Use is Widespread and Protection Could be Improved*, GAO-07-1023T, June 21, 2007, http://www.gao.gov/new.items/d071023t.pdf.

[86] Social Security Administration, Office of the Inspector General, *Removing Social Security Numbers From Medicare Cards*, A-08-08-18026, May 2008, p. 1, http://www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf.

[87] Ibid., p. 3.

[88] 42 U.S.C. §13925.

The Government Accountability Office (GAO) has identified vulnerabilities in federal laws protecting personally identifiable information—and specifically, SSNs—across industries. For one, some industries, such as the financial services industry, have more restrictions on safeguarding this information, while information resellers are not covered by the same restrictions.[89] In order to reduce discrepancies across industries, one policy option may be to provide certain federal agencies with authority to curb the prevalence of SSN use in the private sector; for example, the GAO has recommended that Congress provide the SSA with the authority to enact standards for uniformly truncating SSNs so that the entire nine-digit numbers are not as readily available.[90] A similar option may be to provide the Attorney General, the FTC, or the SSA with the authority to set rules and standards for the sale and purchase of SSNs.

Others have suggested that policies should be focused on *eliminating* the use of SSNs as authenticators rather than on *securing* their use. The premise is that SSNs are often public information and, if not already available, they can be predicted with relative ease.[91] For instance, researchers have demonstrated how the public availability of names and birth data allow for SSN predictability and subsequent vulnerability. As such, some have recommended that efforts not be focused on securing SSNs that are often already public and predictable. Rather, they have suggested that private sector entities abandon the SSN in favor of an alternative identity authenticator.[92]

Effects of Data Breaches

One issue that Congress may consider involves the relationship between data breaches and identity theft. Although there is not a large body of research examining this relationship, existing data suggest that between 12%[93] and 27%[94] of identity theft incidents may result from data breaches. However, this proportion is truly unknown because most victims of identity theft do not know precisely how their personally identifiable information was acquired. In order to prevent any proportion of identity theft that may result from data breaches, or to mitigate the extent of the damage resulting from breach-related identity theft, Congress may wish to consider whether to strengthen data breach notification requirements. Such requirements could affect both the notification of the relevant law enforcement authorities as well as the notification of the individual whose personally identifiable information may be at risk from the breach.

Proponents of increasing breach notification requirements point to research on recent trends in identity theft and the resulting monetary loss. As mentioned, the sooner people become aware that they are victims of identity theft, the faster they take compensatory steps to mitigate the

[89] U.S. Government Accountability Office, *Social Security Numbers: Use is Widespread and Protection Could be Improved*, GAO-07-1023T, June 21, 2007, pp. 12-13, http://www.gao.gov/new.items/d071023t.pdf.

[90] Ibid.

[91] See, for example, Alessandro Acquisti and Ralph Gross, "Social Insecurity: The Unintended Consequences of Identity Fraud Prevention Policies," http://www.heinz.cmu.edu/~acquisti/papers/acquisti-MISQ.pdf.

[92] Ibid.

[93] Synovate, *Federal Trade Commission: 2006 Identity Theft Survey Report*, November 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[94] Gary R. Gordon, Donald J. Rebovich, and Kyung-Seok Choo, et al., *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, Center for Identity Management and Information Protection, Utica College, OJP, BJA Grant No. 2006-DD-BX-K086, October 2007, http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

damage.[95] Proponents also argue that placing enhanced reporting requirements on industries may influence businesses to increase their data security standards, which could, in effect, decrease data breaches and any possibly resulting identity theft.[96] On the other hand, opponents of increasing notification requirements point to research suggesting that the percentage of data breaches that result in identity theft could be less than 1%, as previously discussed.[97] Opponents may then argue that the costs that businesses could incur from increased notification (in terms of dollars and personnel time) could thus exceed the costs incurred by potential identity theft victims from the small proportion of data breaches that may actually result in identity theft.

In addition to strengthening post-breach notification requirements, another policy option aimed at decreasing data breach-related identity theft involves strengthening data security. Several options to reduce the availability of personally identifiable information were discussed in the preceding section. However, a broader data security issue concerns overall information security. Because many incidents of identity theft may occur over the Internet, enhancing cyber security measures could reduce the incidents of identity theft.[98]

Deterrence and Punishment

As mentioned, identity theft is broadly defined in current law. This is in part because it is a facilitating crime, and the criminal act of stealing someone's identity often does not end there. Consequently, investigating and prosecuting identity theft often involves investigating and prosecuting a number of related crimes. In light of this interconnectivity, the President's Identity Theft Task Force recommended expanding the list of predicate offenses for aggravated identity theft, as discussed earlier.[99] The task force specifically suggested adding identity theft-related crimes such as mail theft,[100] counterfeit securities,[101] and tax fraud.[102] However, the task force did not cite specific data to support the claim that these specifically mentioned crimes are in fact those most often related to (either facilitating or facilitated by) identity theft. If Congress considers expanding the list of predicate offenses for aggravated identity theft, it may request that the U.S. Attorneys as well as the appropriate investigative agencies (e.g., FBI, USSS, ICE, and USPIS) provide a report detailing the relationship between identity theft and other federal crimes not yet codified as predicate offenses. A second question that Congress may raise if it considers

[95] Javelin Strategy & Research, "Latest Javelin Research Shows Identity Fraud Increased 22 Percent, Affecting Nearly Ten Million Americans: But Consumer Costs Fell Sharply by 31 Percent," press release, February 9, 2009, http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent/.

[96] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, NH, June 25, 2008, http://weis2008.econinfosec.org/papers/Romanosky.pdf.

[97] Findings from Javelin Strategy & Research cited in Ben Worthen, "Cardholders Buy Peace of Mind, If Not Security," *The Wall Street Journal*, March 10, 2009, p. D1.

[98] A complete discussion of relevant cyber security issues is outside the scope of this report. However, see CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna C. Henning for a discussion of current issues in cyber security.

[99] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007, at http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[100] 18 U.S.C. §1708.

[101] 18 U.S.C. §513.

[102] 26 U.S.C. §7201, 7206-7207.

expanding the list of predicate offenses regards which identity theft-related crimes may most affect national priorities such as economic health and national security.

As more information is stored online by individuals and organizations, there is a risk that online identity thieves may take advantage of this large body of data. And there need not be an increasing number of data breaches in order for criminals to reach a large pool of information. For instance, while the number of reported data breaches decreased in 2009, the number of records impacted spiked over previous years, as illustrated in **Figure 5**. As mentioned, the range of potential victims includes not only individuals but organizations as well. The task force cites "phishing" as a means by which identity thieves assume the identity of a corporation or organization in order to solicit personally identifiable information from individuals.[103] For reasons such as this, the task force recommended that Congress clarify the identity theft and aggravated identity theft statutes to cover both individuals and organizations targeted by identity thieves.

Selected Legislation from the 112th Congress

Several pieces of legislation introduced in the 112th Congress would address the trends in identity theft. The proposals would provide for measures to safeguard information and persons possibly at risk for identity theft.

Social Security Numbers

Legislation was proposed to secure Social Security numbers (SSNs) as well as to minimize the public availability of these numbers. Proposals include prohibiting the display of SSNs on Medicare, Medicaid, or Children's Health Insurance Plan (CHIP) identification cards.[104] Other proposals would require the Commissioner of Social Security to issue a new SSN to a child whose account number has been stolen.[105] Policymakers also proposed legislation to prevent unauthorized access to information contained in the Social Security Death Master File.[106]

Legislation was introduced that would require the Attorney General and the Comptroller General to report to Congress on the uses of Social Security numbers as well as the prevalence of Social Security numbers in public records.[107]

Law Enforcement and Consumer Notification

Legislation introduced in the 112th Congress would enhance both law enforcement and consumer notification of suspected identity theft. For example, some proposals would require the Secretary of the Treasury to notify the FBI as well as the potential victim if there is substantial likelihood

[103] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007, pp. 91-92, at http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[104] See the Seniors' Identity Protection Act of 2011 (H.R. 978), the Medicare Identity Theft Prevention Act of 2011 (H.R. 1509), and the Social Security Number Protection Act of 2011 (S. 1275).

[105] See the Social Security Child Protection Act of 2011 (H.R. 3008).

[106] See the Tax Crimes and Identity Theft Prevention Act (H.R. 3482) and the Identify [sic] Theft and Tax Fraud Prevention Act (H.R. 3215, S. 1534).

[107] See, for example, the Protecting the Privacy of Social Security Numbers Act (S. 1199).

that the individual's social security account number was fraudulently used in the employment context.[108] Still others would require the agency or business entity wherein a data breach occurred to notify law enforcement, the FTC, and the individuals whose personally identifiable information may have been compromised.[109]

Author Contact Information

Kristin M. Finklea
Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259

[108] See H.R. 1538, the Social Security Identity Defense Act of 2011.

[109] See the Data Accountability and Trust Act (H.R. 1707), the Data Accountability and Trust Act (DATA) of 2011 (H.R. 1841), the SAFE Data Act (H.R. 2577), the Personal Data Privacy and Security Act of 2011 (S. 1151), the Data Security and Breach Notification Act of 2011 (S. 1207), the Data Breach Notification Act of 2011 (S. 1408), and the Personal Data Protection and Breach Accountability Act of 2011 (S. 1535).