Identity Theft: Trends and Issues

Updated January 16, 2014

Congressional Research Service
https://crsreports.congress.gov
R40599

CRS REPORT
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 undermine the nation's financial stability. Identity theft is one such crime. In 2012, about 12.6 million Americans were reportedly victims of identity fraud, and the average identity fraud victim incurred a mean of $365 in costs as a result of the fraud. 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 before rising in 2011 and 2012. Identity theft case filings and convictions peaked in 2007 and 2008, and have generally declined since. *Aggravated identity theft* case filings and convictions, on the other hand, have largely continued to increase since aggravated identity theft was added as a federal offense in 2004.

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. Congress may also be interested in assessing the true scope of data breaches, particularly involving government networks.

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, requiring that creditors and financial institutions with specified account types develop and institute written identity theft prevention programs.

Contents

Figures

Contacts

Introduction

Policymakers continue to be concerned with securing the economic health of the United States—including combating those crimes that threaten to undermine the nation's financial stability.[1] Identity theft, for one, poses both security and economic risks. By some estimates, identity fraud cost Americans nearly $21 billion in 2012.[2] Federal Trade Commission (FTC) complaint data indicate that the most common fraud complaint received (18% of all consumer fraud complaints) is that of identity theft.[3] In 2012, for instance, about 12.6 million Americans were reportedly victims of identity fraud. This is an increase from the approximately 11.6 million who were victimized in 2011 and 10.2 million who were victimized in 2010.[4] Mirroring this increase in the overall number of reported identity fraud incidents, consumer costs relating to these incidents increased in 2012; the average identity fraud victim incurred a mean of $365.[5] Nonetheless, this cost is about 42% less than the average expense roughly a decade ago.[6]

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.[7] 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 selected 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. It also examines possible issues for Congress to consider.

---

[1] See, for example, U.S. Congress, House Committee on Financial Services, *Cyber Threats to Capital Markets and Corporate Accounts*, 112th Cong., 2st sess., June 1, 2012.

[2] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013.

[3] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December 2012*, February 2013, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

[4] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013.

[5] Ibid.

[6] CRS calculation based on data from Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013; and Javelin Strategy & Research, *2012 Identity Fraud Report: Consumers Taking Control to Reduce Their Risk of Fraud*, February 2012.

[7] 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 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.[8]

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.[9] 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."[10] 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.[11] 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.

Theft vs. Fraud

Identity theft and identity fraud are terms that are often used interchangeably. Identity fraud[12] is the umbrella term that refers to a number of crimes involving the use of false identification—

[8] 18 U.S.C. §1028(a)(7).

[9] 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.

[10] 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))."

[11] 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.

[12] 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.

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 went before the U.S. Supreme Court. The statutory definitions of identity theft and aggravated identity theft indicate that they are crimes when someone "*knowingly* [emphasis added] 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.[13] 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.[14]

Legislative History[15]

Until 1998, identity theft was not a federal crime.[16] Leading up to Congress designating identity theft as a federal crime, identity fraud was on the rise, and the Internet was increasingly being 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;[17] the laws were not keeping up with technology, and stronger laws were needed to

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

[14] Legislation was introduced in the 112th Congress (H.R. 2552, Identity Theft Improvement Act of 2011) that would have amended the identity theft and aggravated identity theft statutes such that in criminal cases, the government would not need to prove that the defendant knew the stolen means of identification belonged to another person.

[15] 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.

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

[17] 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.

investigate and punish identity thieves.[18] 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 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.[19]

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).[20] 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.

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.[21] 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

[18] 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.

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

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

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

awareness of, prevent, detect, and prosecute) identity theft. It was composed of representatives from 17 federal agencies.[22]

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.[23]

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.

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

[22] 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.

[23] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007.

- 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.[24]

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."

Red Flags Rule[25]

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)[26] by directing the FTC, along with the federal banking agencies and the National Credit Union Administration, to develop Red Flags guidelines. These guidelines require

[24] Ibid.

[25] 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.

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

creditors[27] and financial institutions[28] with "covered accounts"[29] 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.[30]

Possible "red flags" could include

- alerts, notifications, or warnings from a consumer reporting agency;
- 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.[31]

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,[32] further extended the compliance date to

[27] Under the Red Flags Rule, a creditor was originally 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 (P.L. 111-319) limited 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." In November 2012, the FTC issued an Interim Final Rule amending the Red Flags Rule definition of a creditor to be in line with the definition outlined in P.L. 111-319.

[28] 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).

[29] 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.

[30] 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.

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

[32] 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.

November 1, 2009,[33] and later to June 1, 2010.[34] The final enforcement date was set at December 31, 2010,[35] 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,[36] 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.[37] 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 about $143 million.[38] 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).[39] 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

[33] 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.

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] 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. For 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.

on patients' willingness to seek medical treatment. The Red Flag Program Clarification Act of 2010 (P.L. 111-319) limited 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 did 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. Any actual effects of the Red Flags Rule—including effects on identity theft rates as well as any indirect consequences—have not yet been evident.[40] Congress may consider monitoring the effects of the impending Red Flags Rule on subsequent identity theft rates.

Trends in Identity Theft

A number of studies have aimed to measure the prevalence of identity theft. Due to a number of factors, including a lack of a consistent definition of identity theft victimization across studies and differing survey populations, there is not a clear understanding of the true scope of identity theft in the United States. For instance, a Bureau of Justice Statistics (BJS) study estimates that 16.6 million U.S. residents were victims of at least one identity theft incident.[41] Another study by Javelin Strategy & Research estimates that in 2012, about 12.6 million Americans were victims of identity theft; this is an increase from the approximately 11.6 million estimated to have been victimized in 2011.[42]

In addition to survey research on identity theft victimization, trends in consumer complaints of victimization provide additional insight into the issue. Similar to the increase in estimated victimization exhibited in surveys, consumer complaints of identity theft to the FTC exhibited a corresponding increase. The FTC received 369,132 consumer complaints of identity theft in 2012, up from 279,156 complaints in 2011.[43] Nonetheless, identity theft incidents reported to the FTC remain a fraction of the estimated victim population. There is a noted difference between the 369,132 complaints received by the FTC in 2012 and survey data indicating that between 12.6 million and 16.6 million people may have actually been 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.

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

[40] CRS has not identified any academic research analyzing the effects of the Red Flags Rule.

[41] Erica Karrell and Lynn Langton, *Victims of Identity Theft, 2012*, U.S. Department of Justice, Bureau of Justice Statistics, NCJ 243779, December 2013. The BJS researchers relied upon data from the 2012 Identity Theft Supplement (ITS) to the National Crime Victimization Survey (NCVS). Over 69,800 individuals ages 16 and over responded to the ITS questionnaire.

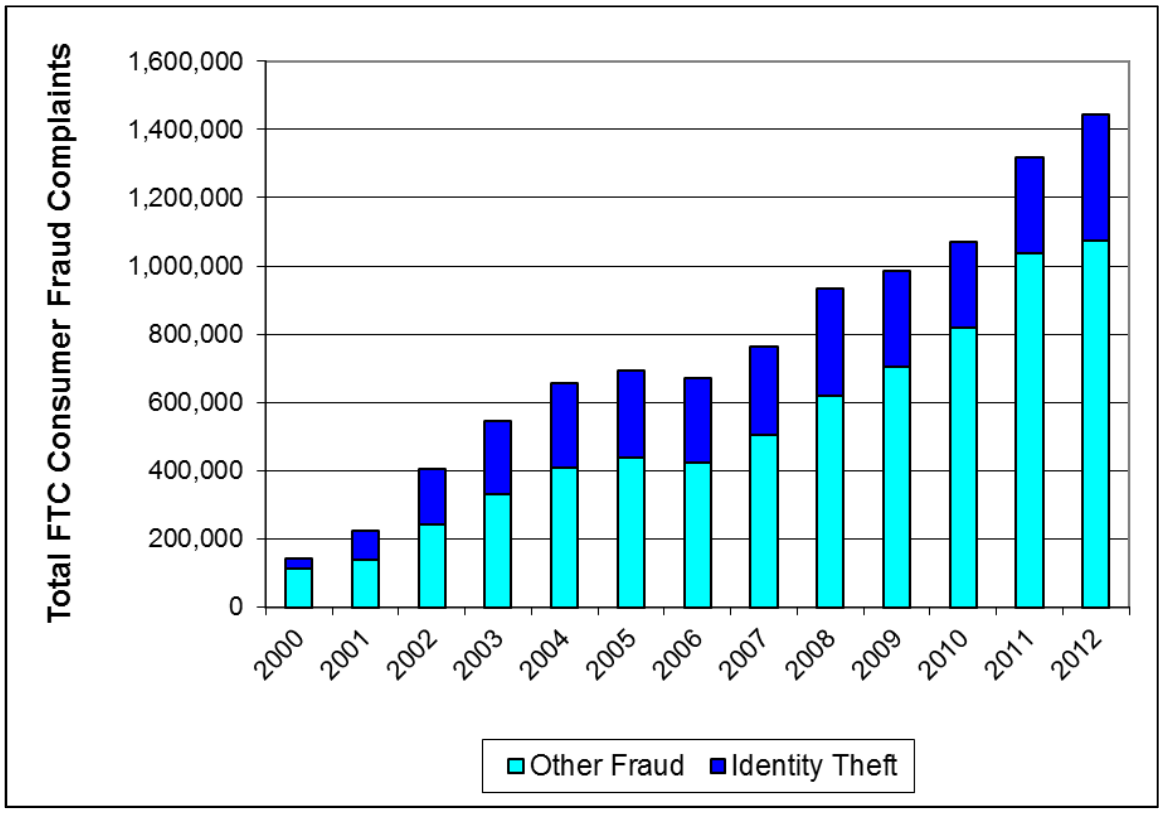
[42] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013.

[43] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December 2012*, February 2013, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

complaints received by the FTC between 2000 and 2012 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 32% of the total number of consumer complaints received by the FTC.[44]

Figure 1. FTC Consumer Complaint Data

Identity Theft and Other Fraud for 2000-2012



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

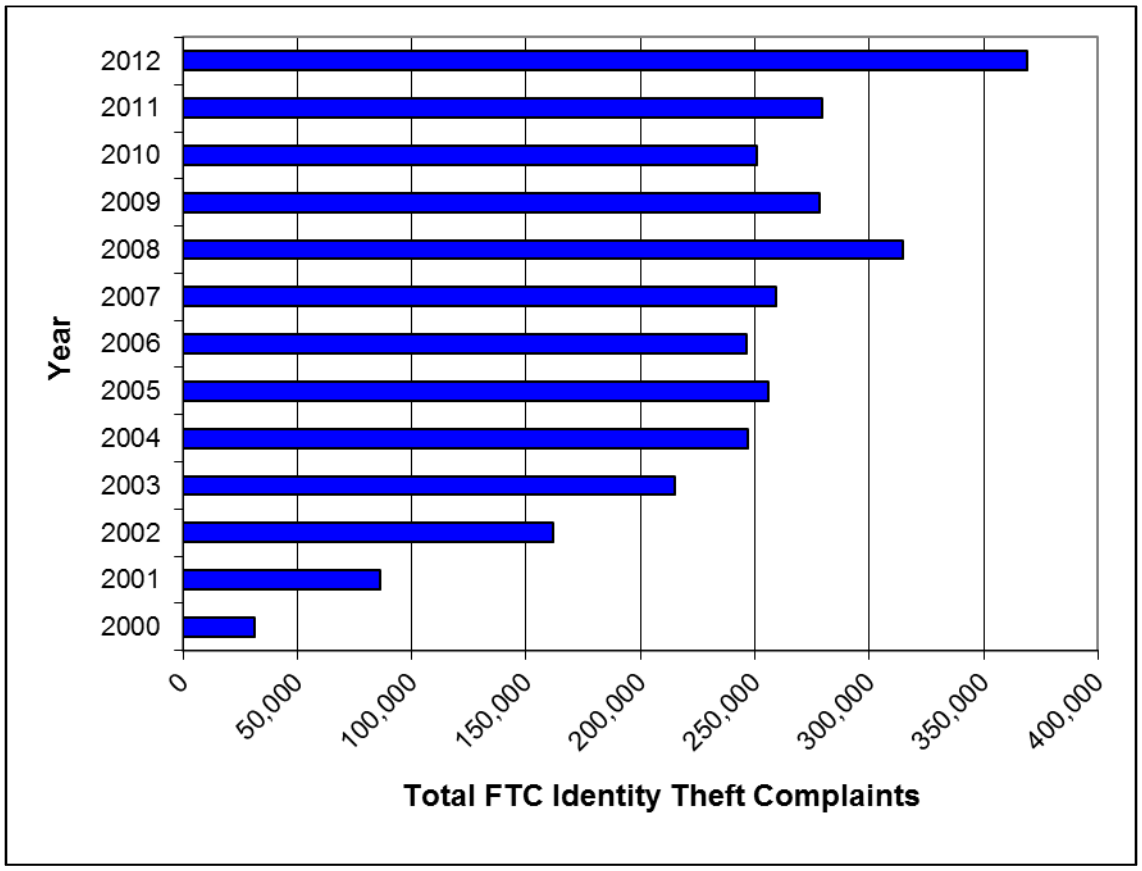
Notes: Data indicate the number of identity theft and other fraud complaints received by the FTC each calendar year. According to CRS analysis, between 2000 and 2012, the number of identity theft complaints has averaged about 32% of the total number of consumer complaints received by the FTC. The percentage 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 before rising again in 2011 and 2012. **Figure 2** illustrates these trends in identity theft complaints reported to the FTC.

[44] Between 2000 and 2012, 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/enforcement/consumer-sentinel-network/reports.

Figure 2. FTC Identity Theft Complaint Data

2000-2012



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

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

Perpetrators

Increasing globalization and the expansion of advanced technology 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.[45] 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.[46] These criminal networks may involve identity thieves located in various cities across

[45] 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.

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

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 and international law enforcement partners, including the U.S. Secret Service, of selected data breaches of businesses around the globe during 2012, 55% of data breaches by external actors—sources outside the compromised organization—were attributed to organized crime.[47] 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.[48]

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, 68% were reported to law enforcement.[49]

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.[50] 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 U.S. Secret Service, the U.S. Postal Inspection Service, 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.

[47] *2013 Data Breach Investigations Report*, Verizon, http://www.verizonenterprise.com/DBIR/2013/. Of note, external actors were involved in 98% of all data breaches.

[48] For a discussion of actor attribution issues related to cybercrime, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

[49] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December 2012*, February 2013, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

[50] 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.[51] 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. 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.[52]

United States Secret Service

The Secret Service serves a dual mission of (1) protecting the nation's financial infrastructure and payment systems to safeguard the economy and (2) protecting national leaders.[53] In carrying out the former part of this mission, the Secret Service 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 43 Financial Crimes Task Forces and 33 Electronic Crimes Task Forces that investigate identity theft, as well as a number of other crimes.[54] In FY2012, the Secret Service arrested 4,277 suspects for crimes related to identity theft, and in FY2013, they arrested 3,868 such suspects.[55]

United States Postal Inspection Service

The U.S. Postal Inspection Service is the federal law enforcement arm of the Postal Service and is the lead federal investigative agency when identity thieves have used the postal system in conducting their fraudulent activities. The most recent Postal Inspection Service data indicate that in FY2012, the Postal Inspection Service sponsored 15 multi-agency task forces across the country that specialized in financial crimes, including identity theft. Further, postal inspectors arrested 627 identity theft suspects—from both Postal Inspection Service investigations and task force investigations in which the Postal Inspection Service was involved.[56] In addition to investigating identity theft, the Postal Inspection Service 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.[57] Examples of victim services include notifying victims of potential identity theft if the Postal Inspection Service discovers compromised identities as well as assisting in victim restitution by providing victims

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

[52] 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 pretenses, such as pretending to be a representative of a financial institution collecting personal information to update financial records.

[53] 18 U.S.C. §3056.

[54] Information provided to CRS by the Secret Service Office of Congressional Affairs, January 10, 2014.

[55] Ibid.

[56] Data provided to CRS by the USPIS Office of Congressional Affairs.

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

money from the funds forfeited as a result of Postal Inspection Service identity theft investigations.[58]

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.[59] 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 these data are transferred to the FTC to be included in their consumer complaint database.[60]

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 2006, ICE created Document and Benefit Fraud Task Forces (DBFTFs). These DBFTFs, located in 19 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.[61]

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 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

[58] U.S. 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.

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

[60] Information provided to CRS by the Social Security Administration, Office of the Inspector General, Office of Congressional Affairs.

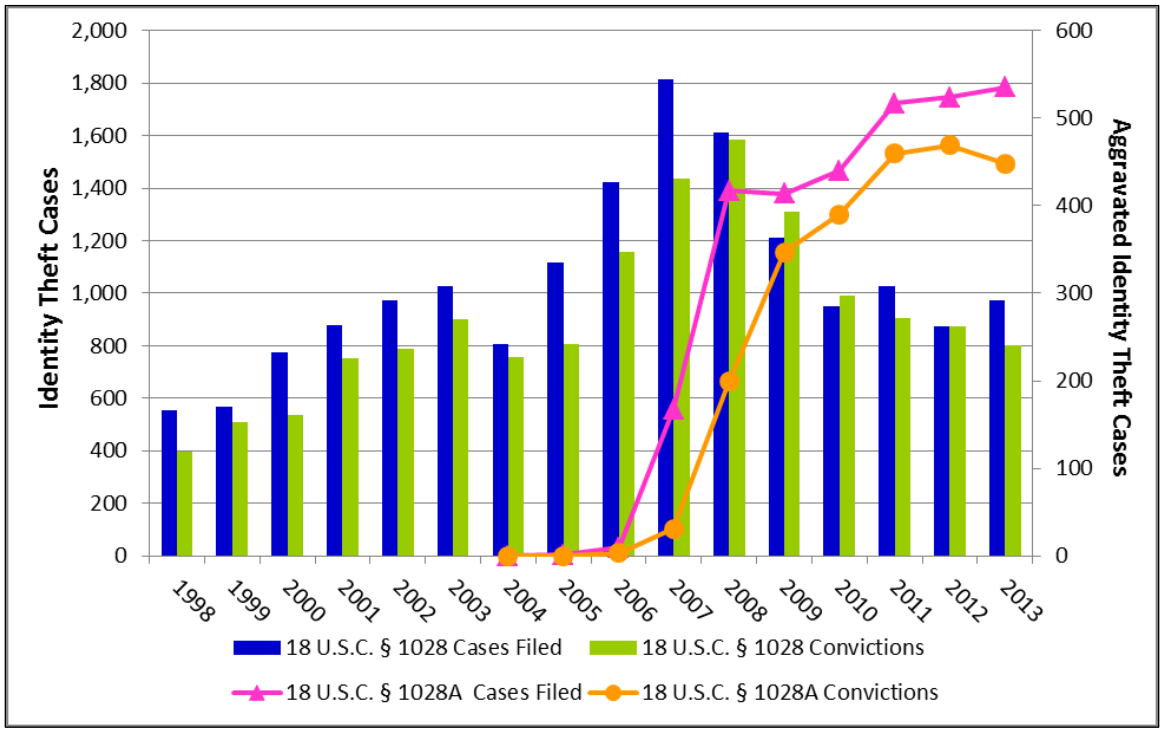
[61] U.S. Immigration and Customs Enforcement, *Document and Benefit Fraud Task Force (DBFTF)*, http://www.ice.gov/document-benefit-fraud/.

tracked by the number of total cases referred to and prosecuted by the USAOs, irrespective of the referring agency.

While the number of identity theft complaints to the FTC has fluctuated over the past several years, so too has 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[62] with the USAOs as well as convictions between FY1998 and FY2013.

Figure 3. Federal Identity Theft and Aggravated Identity Theft Cases

Cases Filed and Case Convictions FY1998-FY2013



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

Notes: Identity theft 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.

The number of identity theft and aggravated identity theft cases *filed* both increased in FY2013 relative to FY2012; conversely, the number of identity theft and aggravated identity theft case *convictions* decreased in FY2013 relative to FY2012 levels. Identity theft case filings and convictions peaked in 2007 and 2008, and have generally declined since. Aggravated identity theft case filings and convictions, on the other hand, have largely continued to increase since aggravated identity theft was added as a federal offense in 2004. Still, if the identity theft and

[62] There may be multiple defendants in a case. Of note, **Figure 3** depicts the number of cases (rather than the number of *defendant* cases) prosecuted and the number of convictions for charges of identity theft and aggravated identity theft for FY1998 through FY2013.

aggravated identity theft data are combined, total case filings and convictions have mostly declined since 2008.

There are several possible explanations for these trends. One possibility is that there has been a decrease in the overall number of actual 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. However, research indicating that the number of individuals victimized by identity thieves is actually continuing to increase, which would suggest this is not a viable explanation.[63] 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, 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 FY2013, while larger than the number filed in FY2012, maintained the largely downward trend beginning in FY2008. 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.

Domestic Impact

As noted, survey data suggest that between 12.6 million and 16.6 million people may have been victimized by identity thieves and fraudsters in 2012.[64] And these are the known cases. The 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.[65] **Figure 4** illustrates the most common misuses of victims' identities.

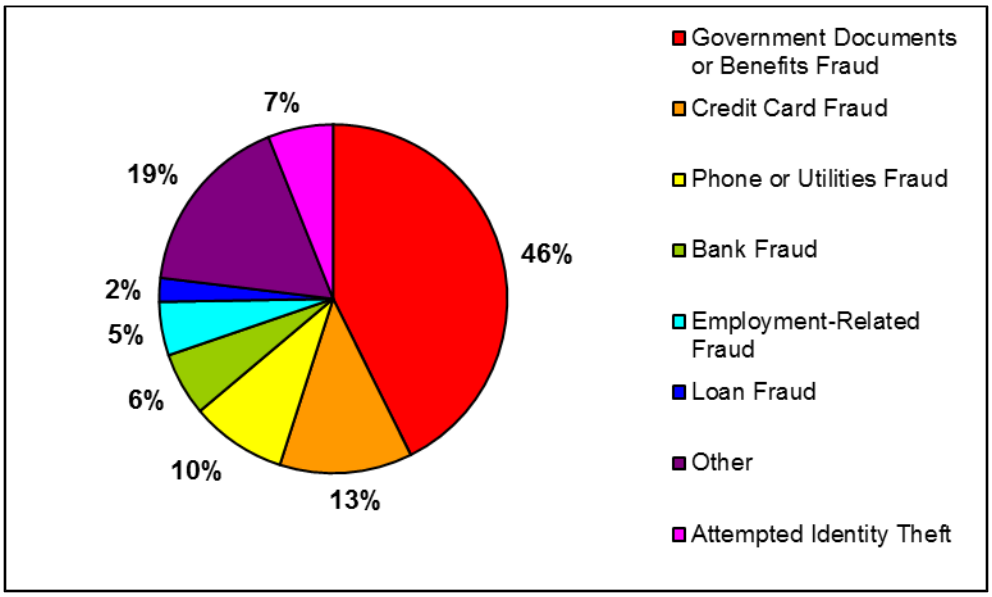
[63] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013; Erica Karrell and Lynn Langton, *Victims of Identity Theft, 2012*, U.S. Department of Justice, Bureau of Justice Statistics, NCJ 243779, December 2013.

[64] Ibid.

[65] 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, 2012

How Victims' Information is Misused



Source: Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December 2012*, February 2013, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

Notes: Of the 369,132 identity theft complaints received by the FTC in 2012, the most prevalent form of identity theft was government documents or benefits fraud. About 11% 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 Internet/email, data breach, evading the law, medical, apartment/house rented, insurance, securities/other investments, property rental fraud, child support, magazines, bankruptcy, miscellaneous, and uncertain. The uncertain subcategory alone accounts for about 8% 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.[66] 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—remaining the leading category in 2012.[67] 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 43% of the identity theft complaints received by the FTC in 2012 and about 24% of these complaints in 2011.[68]

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.

[66] 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.

[67] Federal Trade Commission, *Consumer Sentinel Network Data Book for January–December 2012*, February 2013, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

[68] Ibid.

Credit Card Fraud[69]

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 adversely 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.[70] 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.[71] In September 2013, eight individuals pleaded guilty to charges "relating to the activities of the Armenian Power criminal enterprise," and 51 persons "previously pleaded guilty for their roles."[72]

Document Fraud[73]

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[74] living in the United States or fake passports for people trying to

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

[70] 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.

[71] 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.

[72] Federal Bureau of Investigation, *Eight Defendants Plead Guilty in Los Angeles in Armenian Power Gang Case*, September 11, 2013, http://www.fbi.gov/losangeles/press-releases/2013/eight-defendants-plead-guilty-in-los-angeles-in-armenian-power-gang-case.

[73] 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).

[74] A complete discussion of immigration-related document fraud is outside the scope of this report, but more information can be found in CRS Report RL32657, *Immigration-Related Document Fraud: Overview of Civil, Criminal, and Immigration Consequences*, by Michael John Garcia; and archived CRS Report RL34007, *Immigration Fraud: Policies, Investigations, and Issues*, by Ruth Ellen Wasem.

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 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.[75]

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 September 2013, three defendants pleaded guilty for their roles in "a sophisticated scheme to produce and sell high-quality false identification documents throughout the nation ... generating profits of more than $3 million over several years."[76] The fraudsters, through their illegitimate business, "Novel Design," sold over 25,000 fraudulent driver's licenses throughout the nation. They even outsourced some of the manufacturing of these fake documents to entities in Bangladesh and China.

Employment Fraud

Identity theft can facilitate employment fraud if the thief uses the victim's personally identifiable information to obtain a job. With the recent elevated levels of unemployment,[77] policymakers may wish to monitor trends in employment fraud. This form of fraud could adversely 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

The Identity Theft Resource Center (ITRC) is one organization that tracks data breaches across the nation, and the resulting statistics indicate that the total number of reported data breaches generally increased between 2005 and 2008 and then fluctuated through 2013 (during which year, there were 619 reported breaches).[78] **Figure 5** illustrates this trend. Breaches are recorded across

[75] 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.

[76] Federal Bureau of Investigation, *Three Accused of Operating Fake ID Ring Plead Guilty*, September 4, 2013, http://www.fbi.gov/richmond/press-releases/2013/three-accused-of-operating-fake-id-ring-plead-guilty.

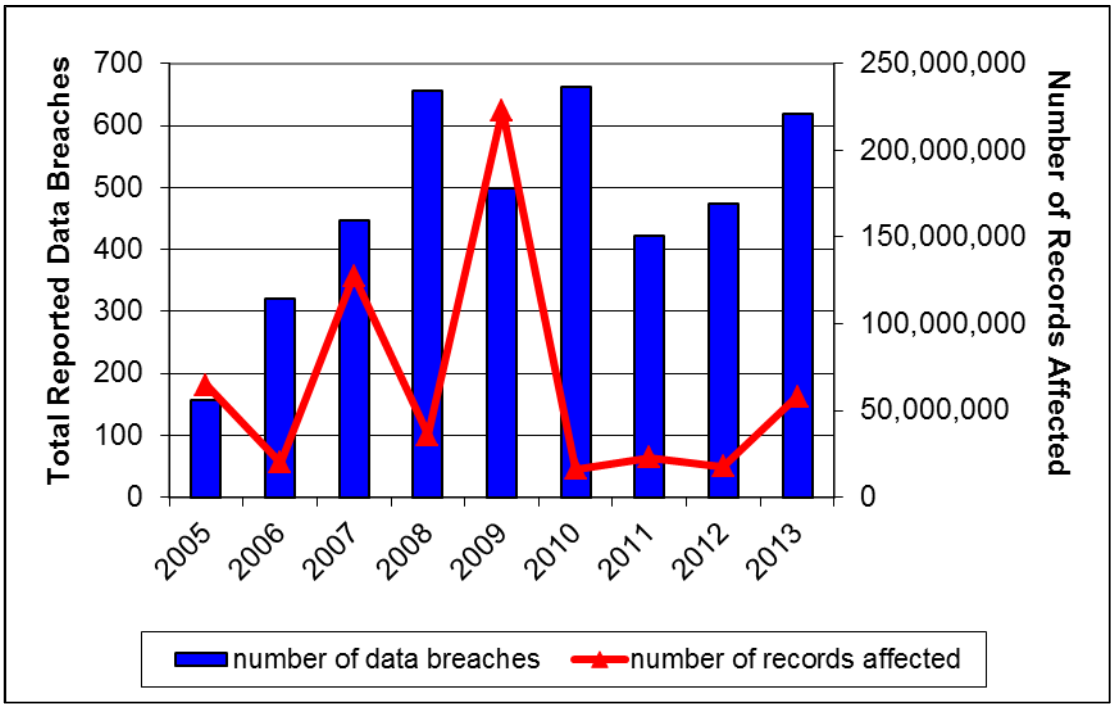
[77] According to the Bureau of Labor Statistics (BLS), the unemployment rate remained at or above 7.0% between December 2008 and November 2013 (peaking at 10.0% in October 2009). In December 2013, the unemployment rate dropped to 6.7%. See http://data.bls.gov/timeseries/LNS14000000.

[78] Identity Theft Resource Center, *2013 Breach Stats*, January 1, 2014, http://www.idtheftcenter.org/images/breach/2013/ITRC_Breach_Stats_Report_2013.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

five industries: banking/credit/financial, business, educational, government/military, and medical/healthcare. In 2013, the medical/healthcare industry experienced the greatest number of data breaches (43.1%) for the first time since the ITRC began tracking this information in 2005 (from 2007-2012, the business sector had filled this top spot). The medical sector was followed in number of breaches by the business (33.9%), government (10.2%), educational (9.0%), and banking (3.7%) sectors.

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

2005-2013



Source: CRS analysis of data provided by the Identity Theft Resource Center, available at http://www.idtheftcenter.org/id-theft/data-breaches.html.

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.[79] California was the first state to enact such legislation in 2002. As of December 2013, 46 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws.[80] The increasing prevalence of state laws requiring breach notification could

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, 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."

[79] 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.

[80] National Conference of State Legislatures, *State Security Breach Notification Laws*, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

lead to an increase in reported breaches to law enforcement, media, or the individuals affected. Nonetheless, the actual number of data breaches remains underreported, and the number of reported breaches does not reflect the 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 2013 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 2013, for example, at least 57,868,922 records were put at risk, but information on the exact number of records exposed was only available for 366 (about 59%) of the 619 reported data breaches.[81] Of note, however, "due to the mandatory reporting requirement for healthcare industry breaches affecting 500 or more individuals, 84% of [the] healthcare breaches publicly stated the number of records exposed."[82]

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.[83] 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. Results from one study note that 25% of surveyed individuals had, at some point, received a "notification about a data breach that involved the loss or theft of their personal information" (and 51% of respondents couldn't recall whether they had received such a notification.[84] And, Javelin Strategy & Research data suggest that nearly one in four (22.5%) individuals receiving breach notifications became victims of fraud.[85]

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 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.[86]

---

[81] Identity Theft Resource Center, *2013 Breach Stats—Known vs. Unknown Totals*, January 1, 2014, http://www.idtheftcenter.org/images/breach/2013/KnownvsUnknownSummary2013.pdf.

[82] Identity Theft Resource Center, *2013 Data Breaches*, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html.

[83] 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.

[84] Ponemon Institute LLC, *2012 Consumer Study on Data Breach Notification*, Sponsored by Experian Data Breach Resolution, June 2012, p. 3.

[85] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013.

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

Synovate conducted a similar study on behalf of the FTC 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.[87] The Center for Identity Management and Information Protection at Utica College evaluated identity theft cases handled by the U.S. Secret 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.[88]

It appears that the stronger relationship between identity theft and data breaches is found when analyzing identity theft victims whose data were 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.[89] 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

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

[88] 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.

[89] 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.

crimes. When policymakers consider the federal government's role in preventing identity theft, they necessarily consider the government's role in preventing interrelated crimes.

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.[90]

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.[91] There are few restrictions on the use of SSNs in the private sector, and therefore the use of SSNs is widespread.[92] 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 2013, approximately 50 million Medicare cards displayed Social Security numbers, potentially placing these individuals at risk for identity theft.[93] Opponents of such legislation may cite that transitioning to a different Medicare identifier has most recently been estimated to cost between $255 million and $317 million.[94]

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.[95] 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

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

[91] 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.

[92] 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.

[93] U.S. Government Accountability Office, *Medicare Information Technology: Centers for Medicare and Medicaid Services Needs to Pursue a Solution for Removing Social Security Numbers from Cards*, GAO-13-761, September 2013, p. 2.

[94] Ibid., p. 14.

[95] 42 U.S.C. §13925.

the use of SSNs—and more specifically, whether it should set limitations as part of eligibility requirements for federal assistance.

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.[96] 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, GAO has recommended that Congress provide SSA with the authority to enact standards for uniformly truncating SSNs so that the entire nine-digit numbers are not as readily available.[97] 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.[98] 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.[99]

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%[100] and 27%[101] 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

[96] 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.

[97] Ibid.

[98] 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.

[99] Ibid.

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

[101] 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.

they are victims of identity theft, the faster they take compensatory steps to mitigate the damage.[102] 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. Results from one study suggest that the adoption of state-level data breach disclosure laws could reduce the identity theft from these breaches by, on average, 6.1%.[103] 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.[104] 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.[105]

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.[106] The task force specifically suggested adding identity theft-related crimes such as mail theft,[107] counterfeit securities,[108] and tax fraud.[109] 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

[102] 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/.

[103] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis & Management*, vol. 30, no. 2 (April 1, 2011), pp. 256-286.

[104] 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.

[105] A complete discussion of relevant cyber security issues is outside the scope of this report. However, see CRS Report R42507, *Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan as a resource for relevant CRS products.

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

[107] 18 U.S.C. §1708.

[108] 18 U.S.C. §513.

[109] 26 U.S.C. §7201, 7206-7207.

not yet codified as predicate offenses. A second question that Congress may raise if it considers 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. As illustrated in **Figure 5**, the number of reported data breaches does not necessarily trend with the number of potentially exposed records. 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.[110] 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.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer

[110] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 23, 2007, pp. 91-92.

Congressional Research Service
Informing the legislative debate since 1914

SBA Disaster Loan Credit Standards, Collateral Requirements, and Debt Collection

May 27, 2026

Congressional Research Service
https://crsreports.congress.gov
R48959

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SBA Disaster Loan Credit Standards, Collateral Requirements, and Debt Collection

SUMMARY

R48959

May 27, 2026

Anthony A. Cilluffo
Analyst in Public Finance

Bruce R. Lindsay
Specialist in American National Government

Maria Kreiser
Senior Research Librarian

The U.S. Small Business Administration (SBA) provides low-interest, long-term loans to disaster survivors to allow them to repair or replace uninsured or underinsured property. About 80% of SBA disaster loans are made to individuals, either for real property damage (such as that to a house) or for personal property damage (such as that to a vehicle or other personal belongings). The other 20% of disaster loans are made to businesses and private nonprofit organizations, either to cover physical damage to business property or to cover financial obligations that could have been met had the disaster not occurred.

In designing the disaster loan program, Congress and the SBA have sought to balance "sympathetic consideration" of the needs and circumstances of disaster survivors with the need to maintain program integrity and protect the federal government's financial interests. Three key factors in this balance are (1) the credit standards required to obtain a disaster loan; (2) the amount and quality of collateral required to be pledged to secure a disaster loan; and (3) debt collection processes followed after default. Together, credit, collateral, and collection policies are designed to keep loan performance and program losses at levels that are deemed acceptable by Congress and the SBA.

To secure an SBA disaster loan, an applicant must demonstrate that they are reasonably likely to repay the loan. The SBA relies on an applicant's credit score to determine whether the applicant has an acceptable credit history; the applicant's credit score further determines whether the applicant is eligible for a loan, what level of processing is required, and whether the applicant likely has access to credit elsewhere (which determines the loan's interest rate). The applicant's repayment ability is gauged on the applicant's income and existing debt. Besides determining loan eligibility, the applicant's estimated repayment ability contributes to decisions regarding monthly payment amount and loan maturity date. The SBA uses a multistep process for loan applications that is designed to quickly decline applications with clearly unacceptable credit histories or little repayment ability; faster rejections allow the SBA to more quickly refer applicants to the Federal Emergency Management Agency (FEMA) for possible grant assistance.

Disaster loan applicants may be required to pledge specific assets as collateral for their loan. In the event of default, the SBA can seize and liquidate this collateral to repay the loan. Requiring more collateral for a loan may increase the likelihood that the SBA will be repaid or, after default, increase the amount the SBA is able to recover. However, higher collateral requirements may reduce access to the program by preventing applicants with insufficient collateral from accessing SBA disaster loans. Currently, disaster loans of $50,000 or less made for a *presidentially* declared major disaster do not require collateral. For disasters receiving declaration by the *SBA Administrator*, loans of $14,000 or less do not require collateral. For SBA home disaster loans that require collateral, the SBA's collateral requirements are more lenient than those of most private lenders. For these loans, the SBA typically takes the borrower's house as the only collateral, regardless of the house's available equity.

SBA business disaster loans have higher collateral requirements compared with SBA disaster loans for individuals or households. Businesses generally must have collateral with available equity at least equal to the value of the disaster loan. Business disaster loans also often require personal guarantees from business principals. Congress and the SBA have, at times, changed the dollar-value threshold above which borrowers are required to pledge collateral; usually, they have increased the threshold. Stated justifications for the changes—when provided—often mention the need to account for inflation occurring since the last change, or a desire to simplify the program.

In the case of loan default and liquidation of collateral, debt collection represents the last opportunity for the federal government to recover its capital. Before a loan defaults, the SBA uses a variety of tools, including financial hardship relief and loan modifications, to help borrowers return to making regular monthly payments. If those options fail, the SBA can refer the loan to the Department of the Treasury for enhanced debt collection efforts, including offsetting (holding back) the borrower's wages or federal payments to the borrower (such as federal tax refunds, contractor payments, or Social Security benefits). A borrower who defaults on an SBA disaster loan also becomes ineligible for most federal loans in the future.

Contents

Tables

Contacts

Introduction

The U.S Small Business Administration (SBA) has been a major source of disaster assistance since the agency was established in 1953. The SBA disaster loan program offers direct, low-interest, long-term loans for physical and economic damages to businesses, nonprofit organizations, and small agricultural cooperatives. The SBA also provides disaster loans to individuals and households.[1]

The SBA disaster loan program provides two types of disaster loans to small businesses and nonprofit organizations:

1. **Business physical disaster loans** provide businesses located in a declared disaster area with up to $2 million[2] to repair or replace damaged physical property, including machinery, equipment, fixtures, inventory, and leasehold improvements[3] that are not covered by insurance.
2. **Economic injury disaster loans (EIDLs)** provide businesses located in a declared disaster area with up to $2 million[4] to help meet financial obligations and operating expenses that could have been met had the disaster not occurred. EIDL proceeds can be used only for the working capital necessary to enable the business or organization to alleviate the specific economic injury and to resume normal operations. EIDL amounts are based on actual economic injury and financial needs, regardless of whether the business suffered any property damage.

Business physical disaster loans and EIDLs are collectively referred to as "SBA business disaster loans."

The SBA disaster loan program also provides two types of disaster loans to individuals and households:[5]

1. **Personal property disaster loans** provide creditworthy homeowners or renters located in a declared disaster area with up to $100,000 to repair or replace their damaged personal property.
2. **Real property disaster loans** provide creditworthy homeowners located in a declared disaster area with up to $500,000 to repair or restore their primary residence to its pre-disaster condition.

Personal property disaster loans and real property disaster loans are collectively referred to as "SBA home disaster loans."

[1] For more information about the Small Business Administration (SBA) disaster loan program, see CRS Report R44412, *SBA Disaster Loan Program: Frequently Asked Questions*, by Bruce R. Lindsay.

[2] The SBA can waive the $2 million maximum amount and provide a larger business physical disaster loan if the business is a major source of employment in the area and meets other requirements. See 15 U.S.C. §636d.

[3] Leasehold improvements are changes that a tenant makes to a commercial rental property to customize the property to the tenant's needs.

[4] The SBA can waive the $2 million maximum amount and provide a larger economic injury disaster loan (EIDL) if the business is a major source of employment in the area and meets other requirements. See 15 U.S.C. §636d.

[5] See the SBA's regulations for Home Disaster Loans (13 C.F.R. §§123.100-123.108); Physical Disaster Business Loans (13 C.F.R. §§123.200-204); and Economic Injury Disaster Loans (13 C.F.R. §123.300-123.303).

Historically, the majority of disaster loans provided by the SBA (roughly 80%) are for individuals and households.[6]

If the amount of an SBA disaster loan is above a certain threshold, an applicant must pledge collateral such as real estate, personal property, or other items of ascertainable value to secure the loan. The SBA uses collateral to minimize its risk by ensuring borrowers stay current on their financial commitment. Collateral also helps offset loan default losses. The SBA obtains rights to a borrower's collateral with a security agreement that outlines the steps the SBA may take if the borrower fails to repay the disaster loan. While the SBA will seek to secure any available collateral, it will not reject an applicant solely because the applicant cannot provide collateral to secure their loan.

The SBA typically secures its collateral interest by taking a lien against the applicant's property. The lien is recorded within the county or state in which the property is located.[7] The SBA does not require an applicant to pledge collateral if the loan amount (or aggregate loan amount) does not exceed the unsecured thresholds (also known as unsecured loan limits). The SBA does not require collateral for personal property disaster loans if the applicant does not own real estate (this usually occurs when the applicant is a renter).[8]

Following a disaster loan default, the SBA is required under the Debt Collection Improvement Act of 1996 (P.L. 104-134, as amended) to "maximize collections of delinquent debts owed to the Government by ensuring quick action ... and the use of all appropriate collection tools."[9] For the first several months following a missed payment, the SBA tries to get the borrower back to making regular monthly payments. Beyond the first few months after a missed payment, the SBA may begin debt collection efforts, including by liquidating collateral and referring the borrower to the Department of the Treasury.[10]

This report first provides an overview of SBA disaster loan budgeting, credit standards, and loan collateral requirements. As discussed later in this report, the amount of collateral required for a disaster loan depends on (1) what type of declaration is issued for the incident, and (2) the total amount of the disaster loan. This report then transitions to discussion of the SBA's policy for debt collection. For the purposes of this report, debt collection occurs when the borrower has become delinquent in making payments on their SBA disaster loan.

Overview of SBA Disaster Loan Budgeting[11]

Budgeting for the SBA disaster loan program is governed by the Federal Credit Reform Act of 1990 (FCRA; Subtitle B of Title XIII of P.L. 101-508). Under FCRA, the SBA records the expected lifetime cost of a disaster loan in the fiscal year that the loan is obligated. This amount,

[6] U.S. Congress, House Committee on Small Business, *Small Business Administration Disaster Assistance Program*, 2017, p. 1. More SBA disaster assistance was provided to small businesses than individuals and households in response to the economic impact of the Coronavirus disease 2019 (COVID-19). For more information about SBA disaster assistance for COVID-19, see CRS Report R46284, *COVID-19 Relief Assistance to Small Businesses: Issues and Policy Options*, by Bruce R. Lindsay, Adam G. Levin, and R. Corinne Blackford.

[7] The SBA sends a letter to the senior lien holder requesting advance notice of any foreclosure actions against the borrower if the lien is located in a "non-notice" state.

[8] Renters who own real estate are required to pledge the real estate as collateral for the loan.

[9] 31 U.S.C. §3701 note.

[10] SBA, *Disaster Loan Servicing and Liquidation*, SOP 50 52 2, September 1, 2015, https://www.sba.gov/sites/default/files/files/SOP_50_52_2_1.pdf (hereinafter SBA SOP 50 52 2).

[11] This section is largely drawn from CRS Report R48558, *SBA Disaster Loans Program Account: Overview and Policy Options*, by Bruce R. Lindsay and Anthony A. Cilluffo.

also known as a *credit subsidy*, is the amount by which the federal government's disbursements exceed amounts received over the loan's lifetime (on a net present value basis).[12] This calculation is largely based on assumptions about the difference between the federal government's cost of borrowing funds and the interest rate charged to disaster loan borrowers; the expected disaster loan default rate; and how much of the defaulted balance the government will eventually recover.[13] At the estimated FY2026 subsidy rate of 18.75%, $1 of credit subsidy appropriations can support $5.33 (or $1 divided by 0.1875) of disaster loan lending.

At times, Congress and the SBA have expressed interest in reducing the cost of a given amount of lending in the disaster loan program. There are two broad options for doing so: (1) reducing the interest rate subsidy, or (2) reducing the cost of defaults, net of recoveries.[14] As shown in **Table 1**, the component of the subsidy rate related to the interest rate has varied from FY2016 to FY2026, from -3.88% to 15.67%, largely based on the external interest rate environment. For more about interest rates in the disaster loan program, see CRS Report R46963, *SBA Disaster Loan Interest Rates: Overview and Policy Options*, by Bruce R. Lindsay, Darryl E. Getter, and Anthony A. Cilluffo.

Compared with the interest rate component, the cost of the defaults component of the subsidy rate (net of recoveries) has varied less over the FY2016 to FY2026 period, ranging from 9.70% to 13.64%, as shown in **Table 1**. Assumptions about the lifetime default rate for the cohort (the group of loans made during a fiscal year) and the post-default recovery rate determine this portion of the subsidy rate. The program's credit policy is the largest contributor to the default rate, while collateral requirements and debt collection policies contribute to the post-default recovery rate. The remainder of this report examines each of these three policy areas in detail.

Table 1. SBA Disaster Loan Credit Subsidy Rates and Loan Assumptions, FY2016-FY2026

Numbers Are Percentages

Fiscal Year	Initial Subsidy Rate Estimate	Components of Subsidy Rate			Loan Assumptions		
		Defaults, Net of Recoveries	Interest Subsidy	All Other	Borrower Interest Rate	Default Rate	Post-Default Recovery Rate
2026	18.75	10.57	10.16	-1.98	2.90	29.01	30.53
2025	22.22	9.70	15.67	-3.15	3.16	29.57	28.57
2024	20.55	10.34	12.67	-2.46	2.93	28.22	27.76
2023	12.91	11.57	1.66	-0.32	2.23	25.38	28.69
2022	8.96	12.61	-3.88	0.23	1.82	25.68	32.01
2021	8.92	11.22	0.72	-3.02	2.23	24.82	29.89
2020	13.62	10.35	7.58	-4.31	2.91	26.11	24.57

[12] A net present value basis calculation adjusts for time differences in the value of money. Generally, due to factors such as inflation and the possibility of earning interest on savings, a dollar is worth more today than it will be far into the future.

[13] A hypothetical loan with no default risk that charges an interest rate similar to the Treasury's cost of borrowing would have no subsidy cost. Disaster loans differ from this hypothetical by both (1) having an interest rate below the Treasury's cost of borrowing and (2) having a default rate above zero.

[14] Alternatively, if Congress or the SBA wanted to expand access to the disaster loan program by making programmatic changes, then this budgetary analysis could help guide an analysis of the potential budgetary costs of those changes.

Fiscal Year	Initial Subsidy Rate Estimate	Components of Subsidy Rate			Loan Assumptions		
		Defaults, Net of Recoveries	Interest Subsidy	All Other	Borrower Interest Rate	Default Rate	Post-Default Recovery Rate
2019	12.29	12.74	2.56	-3.02	2.67	27.85	23.22
2018	12.54	13.01	3.45	-3.91	2.73	28.51	21.59
2017	14.42	13.30	5.62	-4.49	2.81	29.65	19.81
2016	12.10	13.64	2.56	-4.11	2.90	27.88	18.13

Source: Table created by CRS using data from President's Budget, Federal Credit Supplements, FY2017-FY2026, available at https://www.govinfo.gov/app/collection/budget/. Each fiscal year is from the following fiscal year's budget document (for example, FY2016 data are from the FY2017 President's Budget), except FY2026, which is from the FY2026 President's Budget.

Notes: SBA = Small Business Administration. The initial subsidy rate estimate is the sum of the three components of subsidy rate. (Any differences are due to rounding.) The initial subsidy rate estimate is estimated before the beginning of the fiscal year and does not incorporate any annual reestimates of the subsidy rate. The initial subsidy rate is the rate used for determining the cost of loans made during the fiscal year, as well as reinstatements of loans for each respective fiscal year after the end of the year. A reinstatement is a loan or part of a loan initially approved in a prior fiscal year that was canceled but subsequently reapproved by the SBA.

SBA Disaster Loan Credit Policy

As a creditor, the SBA takes steps to be reasonably sure a loan will be repaid in full. To that end, the SBA requires that the applicant have a "satisfactory credit history," meaning that the applicant's credit history "generally shows payments to creditors as agreed unless otherwise justified."[15] The SBA requires that its loan officers "consider the totality of circumstances affecting the overall credit of the applicant when evaluating credit."[16] Applicants must also be able to afford the additional debt burden of the potential loan to be approved.

Acceptable Credit History

For both individual and business applicants, the credit verification process for a disaster loan generally starts when an SBA loan officer pulls a credit bureau report (such as a report from Equifax, Experian, or TransUnion) for the applicant. An individual loan application will generally use only the credit report of the individual applicant. A disaster loan of $200,000 or more to a business also requires a commercial credit report (such as that from Dun & Bradstreet) prior to a credit worthiness decision.[17]

For individual disaster loan applicants, there are three important credit score thresholds:

1. An applicant with a credit score below the SBA's minimum acceptable score is automatically declined. As of November 2023, the SBA uses a minimum acceptable credit score of 570.[18] According to the U.S. Government

[15] SBA, *Disaster Assistance Program*, SOP 50 30 9, May 31, 2018, p. 87, https://www.sba.gov/sites/default/files/2018-06/SOP%2050%2030%209-FINAL.PDF (hereinafter SBA SOP 50 30 9).

[16] SBA SOP 50 30 9, p. 87.

[17] SBA SOP 50 30 9, p. 87.

[18] U.S. Government Accountability Office (GAO), *Disaster Loan Program: SBA Should Include Key Issues in Its Review of How the Program Affects Underserved Communities*, GAO-24-106682, November 30, 2023, p. 11, https://www.gao.gov/products/gao-24-106682.

Accountability Office (GAO), the SBA has reported that it "automatically declines applicants so they can seek assistance from [the Federal Emergency Management Agency (FEMA)] faster."[19] An applicant whose application is automatically rejected due to a low credit score may request that the SBA reconsider their application through a manual review of the applicant's credit report.

2. An applicant with a credit score of 625 or greater with an income of $50,000 per year or greater is eligible for expedited processing.[20] Applicants meeting both requirements are presumed to have repayment ability, allowing them to bypass the fixed debt method for repayment analysis (explained further below).[21]
3. An applicant with a credit score of 700 or greater might be determined to have credit available elsewhere and therefore may have to pay a higher interest rate on their SBA disaster loan.[22]

The SBA is generally willing to consider the totality of circumstances behind adverse credit events, particularly if the events were due to a disaster. Applicants can overcome a poor credit history with reasonable explanations for why the events happened, such as if the events were due to factors outside the applicant's control or if the events were due to temporary factors.[23] Applicants are less likely to be successful in doing so, however, if their credit history includes delinquent federal obligations, such as federal student loans, SBA business loans, previous disaster loans, federal contracts or grants, or other debts owed to the government. Applicants with delinquent federal obligations who do not have a judgment lien against their property may be eligible for a disaster loan, but the loan would require special processing. Applicants with delinquent federal obligations who do have a judgment lien against their property are generally ineligible, but an applicant might be eligible if the delinquency is due to the disaster itself or if the applicant was current on a repayment plan before the disaster.[24]

Repayment Ability

Disaster loan applicants must also demonstrate an acceptable repayment ability to be approved for a disaster loan. For the repayment ability analysis for SBA home disaster loans, there are three key thresholds:

[19] GAO, *Disaster Loan Program*. For more about FEMA assistance for individuals, see CRS In Focus IF11298, *A Brief Overview of FEMA's Individual Assistance Program*, by Elizabeth M. Webster.

[20] GAO, *Disaster Loan Program*, p. 8.

[21] SBA SOP 50 30 9, pp. 92-93.

[22] Historically, the SBA's determination of "credit elsewhere" had three parts; applicants were determined to have reasonable credit available elsewhere if they passed at least two of the three tests. One of those tests is having a credit score of 700 or greater. Another test is related to whether the applicant's available cash flow is significantly greater than the expected loan payment. The third test is whether the applicant's pre-disaster adjusted net worth (assets minus liabilities, with a $100,000 deduction) is more than four times greater than the uncompensated loss. The SBA amended its regulations in July 2024 to remove the cash flow and net worth tests, allowing the agency to base the credit elsewhere test entirely on the applicant's credit score. The SBA has not updated the program SOPs for that change, so it is not clear how the SBA implemented the change or if it is still using the 700 credit score threshold. See SBA, "Disaster Assistance Loan Program Changes to Unsecured Loan Amounts and Credit Elsewhere Criteria," 89 *Federal Register* 59826, July 24, 2024, https://www.federalregister.gov/d/2024-16207.

[23] SBA SOP 50 30 9, pp. 87-88.

[24] SBA SOP 50 30 9, pp. 90-91.

1. At the initial interview stage, the SBA *summarily declines*[25] applications from applicants with low income, as they are unlikely to have available cash flow to repay a disaster loan.[26] The SBA also summarily declines applicants with high existing debt relative to their income.[27] In both cases, a shorter time frame for rejection decisions may allow the SBA to refer disaster survivors more quickly to FEMA for potential grant assistance.[28]
2. For applicants who are not summarily declined for low income or high existing debt, the SBA makes an initial estimate of repayment ability based on income as reported on the loan application and total debts from the credit bureau report. If this initial estimate of monthly income available for repayment is less than $50, then the SBA *automatically declines*[29] the application.[30]
3. If the applicant passes the previous two tests and is not eligible for expedited processing (which requires a credit score of at least 625 and an income of at least $50,000 per year), then the SBA assesses repayment ability using the SBA's "fixed debt method" (FDM).[31] The FDM is based on the principle that there is a maximum amount of debt that a person can reasonably afford and that providing debt above that level entails unacceptable risk of default.[32] The test compares monthly gross income to existing debt and an estimate of basic living expenses to determine whether the applicant has enough available cash flow to be able to repay the disaster loan. For individual applicants, the income available for additional debt payments (which helps determine the maximum loan amount and the loan term) is generally monthly gross income (from all recurring sources), less a 25% disregard[33] for living expenses and less monthly payments for housing (rent or mortgage and related expenses), auto loans, credit cards, and other obligations.[34]

The process to determine repayment ability for business disaster loans is different. Business disaster loans are not subject to the summary declination and automatic declination processes. Instead, business applicants are more likely than individual applicants to undergo the full FDM

[25] In the SBA disaster loan program, a *summary decline* is when an application is declined at the intake stage, before it has been accepted for processing.

[26] The low-income threshold is updated by the SBA annually. However, these announcements are not publicly available. For 2017 income levels, see SBA SOP 50 30 9, Appendix 4, p. 165.

[27] SBA SOP 50 30 9, p. 10.

[28] For more about FEMA assistance for individuals, see CRS In Focus IF11298, *A Brief Overview of FEMA's Individual Assistance Program*, by Elizabeth M. Webster.

[29] In the SBA disaster loan program, an *automatic decline* is when an application is declined by the automated checks based on the credit bureau report. These tests occur after an application has been accepted for processing.

[30] SBA SOP 50 30 9, p. 92. Individuals and households with low income may be eligible for FEMA grant assistance. For more information about the application process for FEMA and SBA disaster assistance, see CRS Report R45238, *FEMA and SBA Disaster Assistance for Individuals and Households: Application Processes, Determinations, and Appeals*, by Bruce R. Lindsay and Elizabeth M. Webster.

[31] As mentioned above, an applicant with a credit score of 625 or greater and income of $50,000 or greater is presumed to have repayment ability and is eligible for expedited processing. Applicants who are eligible for expedited processing do not undergo the fixed debt method (FDM) examination.

[32] SBA SOP 50 30 9, p. 96.

[33] In the SBA disaster loan program, the *disregard* is the portion of income that is considered to be unavailable to service a disaster loan. For example, an applicant with $3,000 in monthly income would have $750 (25% of $3,000) disregarded. The test would assume that the applicant has a total of $2,250 ($3,000 minus $750) available each month for housing costs, existing debts, and the SBA disaster loan.

[34] SBA SOP 50 30 9, pp. 96-100.

analysis. For the FDM analysis, business applicants have a 40% disregard rate for their monthly gross income (versus the 25% disregard rate for individual applicants).[35]

Loan Acceptance and Approval Data

A November 2023 GAO analysis examined the outcomes of SBA disaster loan applications submitted by survivors of one of 13 hurricanes that occurred from FY2018 to FY2022.[36] **Table 2** summarizes the outcomes, which are also described below.

Of the 430,158 disaster loan applications submitted, over half (54%) were either summarily declined or were declined after further processing. Around a quarter (about 111,380) of total applicants were summarily declined for having low income, high existing debt, or both. Among the applications that were accepted for processing but later declined, 63,399 applications (15% of all received applications) were declined due to unsatisfactory credit history, and 39,287 (9% of all received applications) were declined due to a lack of repayment ability. These two groups include some overlap, since the SBA can identify multiple reasons for declining an application. The SBA and GAO sources are not clear about how much the groups overlap. Depending on how much overlap there was between these two groups, somewhere between 41% and 50% of total disaster loan applications received following the 13 hurricanes were declined due to an unacceptable credit history, a lack of repayment ability, or both.[37]

Table 2. Outcomes of SBA Disaster Loan Applications

Based on Applications from Survivors of 13 Hurricanes from FY2018 to FY2022

Outcome	Number of Applications	Percent of Applications Received
Applications received	**430,158**	**100%**
Summarily declined for low income, high existing debt, or both	~111,380[a]	26%
Other applications not accepted for processing	~5,862[a]	1%
Applications accepted for processing	312,916	73%
... Total declined (automatic decline or after further review)	120,924	28%
... Unsatisfactory credit history[b]	63,399[c]	15%
... Lack of repayment ability[b]	39,287[c]	9%
... Ineligible business or property[b]	13,176[c]	3%
... Applications withdrawn	59,703	14%
... Applications in progress at the time of GAO's study	911	<1%
... Applications approved	131,378	31%

[35] SBA SOP 50 30 9, p. 96. This higher disregard rate means that a business will qualify for a smaller disaster loan, or would require a longer loan term, than an individual with similar income and existing debts.

[36] GAO, *Disaster Loan Program*.

[37] These shares include applications summarily declined for low income, high existing debt, or both, as well as loans declined during processing for unsatisfactory credit history or lack of repayment ability. Therefore, the number of loans declined for these reasons can range from 174,779 (111,380 plus 63,399, which assumes *all* loans that were declined during processing for lack of repayment ability were also declined for unsatisfactory credit history) to 214,066 (111,380 plus 63,399 plus 39,287, which assumes that *none* of the loans that were declined during processing for unsatisfactory credit history were also declined for lack of repayment ability). The share of total applications thus declined can range from 41% (174,779 divided by 430,158) to 50% (214,066 divided by 430,158).

Source: Table created by CRS based on data in U.S. Government Accountability Office (GAO), *Disaster Loan Program: SBA Should Include Key Issues in Its Review of How the Program Affects Underserved Communities*, GAO-24-106682, November 30, 2023, pp. 21-24, https://www.gao.gov/products/gao-24-106682.

Notes: SBA = Small Business Administration. See the GAO report for additional details on the analysis.

a. These numbers are estimates. GAO states that "most applications (95 percent) that were not accepted [for processing] were summarily declined" (see p. 22 of the GAO report).

b. These are only the top three reasons for an application's decline; other reasons are not listed.

c. The numbers and percentages do not sum to the total and share of loans declined because the SBA can list multiple reasons for declining an application; an application may therefore be counted under multiple categories.

According to GAO's analysis, the average credit score of applicants whose applications were automatically declined for poor credit was 533, while the average credit score of applicants whose applications were approved was 697.[38]

SBA Disaster Loan Collateral Policy

As a provider of disaster assistance, the SBA has decided that it should seek to "sympathetically consider" the needs of the applicant.[39] To that end, the SBA often requires less collateral for a disaster loan than would be required for a similar loan in the private sector. Disaster loans (real property and business physical) that fall below a certain threshold do not require any collateral. For real property disaster loans (typically for homes) above the collateral threshold, the SBA typically takes a lien on the applicant's disaster-damaged house and considers the collateral requirement to be met, regardless of the value of the collateral. Business applicants have stricter collateral requirements. Businesses must pledge collateral with sufficient value to cover the full amount of the loan. Additionally, the business's principals must provide personal guarantees, which may be secured by the principals' personal assets. Congress and the SBA have regularly made changes to these collateral policies over the history of the program, as described below in "Collateral Policy History."

The unsecured loan threshold has a role in determining the loan proceeds that the SBA can provide to borrowers relatively quickly. Loan processing takes longer for borrowers who provide collateral because the SBA must document the collateral and make required legal filings to protect the SBA's interest in the collateral. However, the SBA can advance amounts up to the unsecured threshold to borrowers relatively quickly, after the loan has been approved and accepted but before collateral filings are complete.[40] Therefore, the unsecured loan threshold is often included in policy discussions about the speed of the SBA's response to disasters.

Secured and Unsecured Loans

Whether a loan is secured or unsecured depends upon whether the borrower pledged collateral and, if so, on the value of the collateral in relation to the loan amount. An *unsecured loan* does not have collateral. A *secured loan* has specific pledged collateral (such as a lien on the borrower's house). A *fully secured loan*, such as what the SBA requires for larger business disaster loans, has specific pledged collateral with a value at least equal to the value of the loan. The *unsecured loan threshold* is used interchangeably with *collateral threshold*, and is the highest dollar value disaster loan (based on loan and declaration type) that the SBA will make without requiring the borrower to pledge collateral.

[38] Due to data limitations, these credit score averages are based on disaster loan applications for 11 of the 13 hurricanes considered. GAO, *Disaster Loan Program*, p. 23.

[39] In program guidance, the SBA encourages disaster assistance employees to "balance between protection of the Agency's [financial] interest and sympathetic consideration of the applicant's needs." See SBA SOP 50 30 9, p. 96.

[40] See SBA SOP 50 30 9, pp. 143-144.

Collateral by Loan Type and Declaration Type

Collateral requirements for SBA disaster loans vary by the type of disaster declaration, disaster loan type, and loan amount (see **Table 3**). There are two types of declarations relevant to the SBA disaster loan program—presidential declarations and SBA Administrator declarations.[41] While the SBA does not require collateral for loans below the threshold amounts listed in **Table 3**, it will accept collateral for smaller loans if the applicant voluntarily offers it (which the applicant may choose to do for tax purposes).[42]

Table 3. SBA Disaster Loan Collateral Requirements

Loan Threshold Amounts for Collateral, by SBA Disaster Loan Type and Declaration

Physical Disaster Home and Business Loan		Economic Injury Disaster Loan (EIDL)
Presidential Declaration	SBA Administrator Declaration	Any Declaration
$50,000	$14,000	$50,000

Source: Table created by CRS based on analysis of 13 C.F.R. §123.11.

Note: SBA = Small Business Administration.

Collateral for SBA Home Disaster Loans

The SBA does not require collateral for a home disaster loan

- of $50,000 or less, if the incident is declared a major disaster pursuant to the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act; P.L. 93-288, as amended; 42 U.S.C. §§5121 et seq.);[43] or
- of $14,000 or less, if the incident is declared a disaster pursuant to the Small Business Act (P.L. 83-163, as amended; 15 U.S.C. §§631 et seq.).[44]

As noted above, for most home disaster loans above the collateral threshold, the SBA will take the disaster-damaged property as collateral for the loan. In these cases, the SBA will consider the collateral requirement to be met, regardless of the owner's available equity in the property.[45] Additional collateral requirements may apply in other, limited cases, such as if the borrower uses the loan proceeds to relocate or if the borrower offers other collateral in lieu of the primary

[41] For information about the types of disaster declarations, see CRS Report R44412, *SBA Disaster Loan Program: Frequently Asked Questions*, by Bruce R. Lindsay.

[42] An SBA home disaster loan primarily secured by a lien on the applicant's private residence may qualify for the mortgage interest deduction. For more information, see Internal Revenue Service, *Home Mortgage Interest Deduction*, Pub. 936, October 28, 2025, p. 6, https://www.irs.gov/forms-pubs/about-publication-936.

[43] The Stafford Act authorizes the federal government's primary sources of financial assistance to help state and local governments, and individuals and households, recover and rebuild following an incident. For an overview of various federal disaster assistance programs, see CRS Report R48712, *Federal Disaster Assistance: An Overview of Programs*, coordinated by Maura Mullins.

[44] The Small Business Act authorizes the SBA Disaster Loan Program. The SBA operates the Disaster Loan Program to provide low-interest loans to homeowners, renters, businesses of all sizes, and nonprofit organizations to assist them with recovering from declared disasters.

[45] Available equity is the value of an asset minus any other claims against it. For example, if the owner of a house worth $400,000 has a mortgage with a senior lien on the house with a balance of $250,000, and a home equity line of credit with a junior lien of $50,000, then the available equity in the house is $100,000 ($400,000 minus $250,000 minus $50,000).

residence.[46] The SBA does not require collateral for personal property loans, even above $50,000, if the applicant does not own any real estate.[47]

Because of these standards, most SBA home disaster loans are provided on terms that are less secured when compared with most private lenders' terms. Private lenders require collateral for many types of private loans without government guarantees. For example, a mortgage is secured by the house and an auto loan by the vehicle. Private lenders might require higher standards for collateral than the SBA, such as requiring that the loan be fully secured by collateral (meaning the value of the collateral meets or exceeds the value of the loan). Taking collateral provides the lender with some security in case of loan default, which reduces the net cost of default for the lender. Private lenders sometimes offer some unsecured credit products—such as credit cards and personal loans—that do not require collateral, but those often have significantly higher interest rates than loans with collateral.

The SBA reported that, for the full portfolio of SBA disaster loans (both home disaster loans and business disaster loans) from 2018 to 2023,[48] 41% of approved borrowers did not provide collateral to fully secure the disaster loan; 13% did not have available equity to secure 20% of the loan; and 7% did not have any available equity to secure any portion of the loan.[49] Security rates are likely lower for home disaster loans, since collateral requirements are higher for business loans (as described below); therefore, these figures would likely be higher for home disaster loans if analyzed separately.

Collateral for SBA Business Disaster Loans

The SBA requires more collateral for business disaster loans than for home disaster loans. However, the SBA does not require collateral for a business disaster loan

- of $50,000 or less, if the loan is an EIDL (regardless of declaration type);
- of $50,000 or less, if the loan is for physical damage and the incident is declared a major disaster pursuant to the Stafford Act; or
- of $14,000 or less, if the loan is for physical damage and the incident is declared a disaster pursuant to the Small Business Act.

Generally, in cases where collateral is required, SBA loan officers are required to "determine what collateral is available, and take that collateral which will best secure each loan."[50] Generally, the SBA requires that business borrowers pledge collateral with available equity worth at least 100% of the loan amount. The SBA prefers real estate (especially non-damaged real estate) and fixed assets, such as machinery and equipment, as collateral. Additionally, the SBA requires all principals in the business (such as partners in a partnership or all owners with at least a 20% share in a corporation) to provide personal guarantees of loan repayment. If the business can pledge sufficient business assets to fully secure the loan, then the required personal guarantees can be unsecured. If not, then the guarantors must make secured guarantees, in which they pledge specific personal assets (such as their personal residence) as collateral for the business loan.[51]

[46] SBA SOP 50 30 9, pp. 113-114.

[47] SBA SOP 50 30 9, p. 113.

[48] The SBA source for these data does not clarify whether these are fiscal years or calendar years.

[49] SBA, "Disaster Assistance Loan Program Changes to Unsecured Loan Amounts and Credit Elsewhere Criteria," 89 *Federal Register* 59826, July 24, 2024, https://www.federalregister.gov/d/2024-16207.

[50] SBA SOP 50 30 9, p. 114.

[51] SBA SOP 50 30 9, pp. 114-117.

Collateral for Multiple Disaster Loans

In some instances, a borrower may have more than one SBA disaster loan (e.g., an individual real property loan and an EIDL).[52] The SBA aggregates loan amounts for the same type of loan (treating home and business physical disaster loans as the same type) provided for the same disaster when determining if the loans require collateral. If the total of all physical disaster loans (home and business) is more than $50,000, then collateral is required for all loans, even if the amount of each loan is less than $50,000. The SBA aggregates physical disaster loans separately from EIDLs. For businesses, the SBA treats affiliated businesses as one borrower for this aggregation. The SBA does not aggregate disaster loans with outstanding balances owed by the same borrower from different disasters.[53]

For example, a borrower with a home disaster loan of $30,000 and a business physical disaster loan of $30,000 would require collateral on both loans. A borrower with a business physical disaster loan of $30,000 and an EIDL of $30,000 would not require collateral on either loan. A borrower with a business physical disaster loan of $25,000 from a disaster several years ago and a new home disaster loan of $30,000 from a disaster this year would not require collateral for either loan. All of these examples assume the loans are pursuant to a presidentially declared disaster; the examples would be different for SBA Administrator-declared disasters.

Collateral Policy History

Collateral requirements for the disaster loan program have changed over time as Congress and the SBA have struck different balances between the need to protect the SBA's interest in the loan and "sympathetic consideration" of the disaster survivor's situation. The stated justifications for changes in collateral thresholds—when provided—have often mentioned adjusting the levels for inflation. **Table 4** lists some of the thresholds (explained further below) in effect at different times in the program's history; threshold amounts are listed in nominal dollars, with comparable values in 2025 dollars using three methods of adjusting for price changes.[54]

Table 4. SBA Disaster Loan Collateral Thresholds

Year and Loan Type	Nominal Dollars	2025 Dollars		
		Median Home Sales Price[a]	GDP Deflator	PPI for Construction Materials
1978, all loans[b]	$5,000	$37,032	$19,349	$21,319
1988, physical disaster loans	$10,000	$36,859	$23,449	$29,216
2008, MREIDL	$50,000	$90,100	$73,265	$86,008

[52] Examples include a borrower who needs a physical disaster loan to repair their business and an EIDL for working capital for the same disaster; a borrower who has two or more affiliate businesses that were damaged by the same disaster; and a borrower who has a home and a business damaged by the same disaster.

[53] SBA SOP 50 30 9, pp. 112-113, with updates by CRS for increased unsecured loan threshold amounts.

[54] Several methods of inflation adjustment are economically reasonable in this context. The median home sales price measures changes in the market value of the primary assets (primary residences) used as collateral for disaster loans to individuals. Additionally, most of these loans to individuals are made to repair disaster damage to a primary residence. The gross domestic product (GDP) deflator measures broad price changes in the economy, using prices paid for goods and services by consumers, businesses, and the government. The Producer Price Index (PPI) for construction materials measures changes in the cost of construction materials. Since most disaster loans (both individual and business) are to repair physical damage, the cost of construction materials is one measure of how those costs have changed over time. Other price adjustment measures beyond these three are also possible; these three were chosen for illustration.

Year and Loan Type	Nominal Dollars	2025 Dollars		
		Median Home Sales Price[a]	GDP Deflator	PPI for Construction Materials
2008, physical disaster loans	$14,000	$25,228	$20,514	$24,082
2014, all except MREIDL	$25,000	$36,187	$33,441	$39,393
2024, loans for presidentially declared disasters	$50,000	$49,365	$51,414	$51,429

Source: Table created by CRS based on data from the Federal Reserve Bank of St. Louis, Federal Reserve Economic Data, accessed April 29, 2026: "Median Sales Price of Houses Sold for the United States," https://fred.stlouisfed.org/series/MSPUS; "Gross Domestic Product: Implicit Price Deflator," https://fred.stlouisfed.org/series/GDPDEF; and "Producer Price Index by Commodity: Special Indexes: Construction Materials," https://fred.stlouisfed.org/series/WPUSI012011.

Notes: SBA = Small Business Administration; GDP = Gross Domestic Product; PPI = Producer Price Index; MREIDL=Military Reservist Economic Injury Disaster Loan. All index data are based on annual averages. The changes in the table are illustrative of long-term trends in the program and are not comprehensive of all changes. See accompanying text for explanations of each change and the types of disaster loans to which they apply.

a. This value adjustment is calculated based on the ratio of the collateral threshold and the median sales price for homes. According to the U.S. Census Bureau and U.S. Department of Housing and Urban Development data cited by the Federal Reserve Bank of St. Louis, the median sales price of homes sold was $55,850 in 1978; $112,225 in 1988; $229,550 in 2008; $285,775 in 2014; $418,975 in 2024; and $413,650 in 2025. For example, in 1978, the $5,000 collateral threshold was about 9% of the median home sale price of $55,850. The equivalent amount in 2025 based on this ratio is $413,650 * 9% = $37,032 (calculated before rounding).

b. Senate Report 100-416 does not include a specific year, instead stating "late 1970s." This table uses 1978 for illustration.

As enacted in the 1950s, the Small Business Act did not provide statutory references to a specific dollar value threshold for requiring collateral,[55] and the SBA administratively allowed smaller loans to go unsecured. By the late 1970s, the administrative unsecured loan limit was $5,000.[56]

The Small Business Administration Reauthorization and Amendment Act of 1988 (P.L. 100-590) provided the first statutory threshold for requiring collateral, with physical disaster loans (home and business) of more than $10,000 requiring collateral.[57] The conference report for that act explained that "this increase simply recognizes inflation and will partially compensate for it and also should streamline loan processing and reduce red tape."[58] The SBA kept the collateral threshold for EIDLs at $5,000.

Several changes to disaster loan collateral policy were made in 2008. The Military Reservist and Veteran Small Business Reauthorization and Opportunity Act of 2008 (P.L. 110-186) added a new provision that required collateral for Military Reservist EIDLs of more than $50,000.[59] Later that same year, the Food, Conservation, and Energy Act of 2008 (P.L. 110-246; 2008 farm bill) was enacted, which made two changes to collateral policies.[60] First, it increased the statutory threshold to require collateral for physical disaster loans of more than $14,000 (from $10,000). Second, it

[55] The Small Business Act, P.L. 83-163 and P.L. 85-536.

[56] U.S. Congress, Senate Committee on Small Business, *Small Business Administration Reauthorization and Amendment Act of 1988*, report to accompany H.R. 4174, 100th Cong., 2nd sess., S.Rept. 100-416, July 7, 1988, p. 23.

[57] P.L. 100-590, §122.

[58] U.S. Congress, House of Representatives, *SBA Reauthorization and Amendment Act of 1988: Conference Report*, report to accompany H.R. 4174, 100th Cong., 2nd sess., H.Rept. 100-1029, October 3, 1988, p. 38.

[59] P.L. 110-186, §203.

[60] P.L. 110-246, §12065.

allowed the SBA to increase that threshold "as the Administrator determines appropriate in the event of a major disaster." The committee report for a related earlier bill[61] again framed the increase in terms of inflation: "[The unsecured loan] threshold is not indexed to inflation ..... This bill would raise the level to $14,000 to allow for homeowners and businesses to access additional capital without the need for collateral."[62] The committee report did not include an explanation for granting discretion to the SBA Administrator to increase the threshold for loans made pursuant to a major disaster.[63]

Following Hurricane Sandy in late 2012, President Obama established the Hurricane Sandy Rebuilding Task Force, comprised of the heads of 23 executive branch departments and agencies.[64] As part of the Task Force's charge, it developed a "Rebuilding Strategy" that included a recommendation to "increase SBA's unsecured disaster loan limits and expedite the disbursement of small dollar loans."[65] Pursuant to that recommendation, in April 2014, the SBA increased the collateral threshold for physical disaster loans (home and business) made pursuant to a major disaster to $25,000 (from $14,000) and increased the collateral threshold for EIDLs for all disaster types (except Military Reservist EIDLs) to $25,000 (from $5,000). The collateral threshold for SBA Administrator-declared disasters was still $14,000. In making the change, the SBA pointed to the Task Force's recommendation and noted that "with these increased limits, more businesses, homeowners, and other potential victims that may be impacted by future disasters will receive much-needed small dollar loans more quickly following a disaster";[66] these unsecured loans can follow expedited processing and disbursement procedures since the SBA does not need to process additional documentation for pledged collateral.[67]

In 2015, the Recovery Improvements for Small Entities (RISE) After Disaster Act of 2015 (P.L. 114-88) made two changes to SBA disaster loan collateral policies. First, the act included a provision that clarified that the SBA shall not require a business owner to pledge their personal residence as collateral for a physical business disaster loan or EIDL of $200,000 or less, provided that the owner could substitute other personal assets of equal quality for the full amount of the loan.

---

[61] S. 163 (110th Congress), the Small Business Disaster Response and Loan Improvements Act of 2007.

[62] U.S. Congress, Senate Committee on Small Business and Entrepreneurship, *Small Business Disaster Response and Loan Improvements Act of 2007*, report to accompany S. 163, 110th Cong., 1st sess., S.Rept. 110-64, May 7, 2007, p. 4.

[63] Although the committee report did not mention a rationale for the change, the context of the bill suggests a few possibilities. First, the report mentions that the unsecured loan threshold is not indexed for inflation. Granting discretion to the SBA Administrator to increase the threshold, at least for major disasters, could allow the SBA to administratively address the effects of inflation. Second, the original legislation (S. 163) was part of a succession of efforts (detailed in the introduction of S.Rept. 110-64) by the Senate Committee on Small Business and Entrepreneurship to reform the SBA disaster loan program following the historically destructive hurricanes Katrina and Rita in 2005. Specifically, the bill's report states that "the SBA failed in its mission to respond quickly and effectively to victims' needs in the weeks and months following the hurricanes." Granting authority to the SBA Administrator to increase the collateral threshold could give the SBA increased flexibility to respond to disasters when there is a heightened need to respond quickly, or in cases of exceptionally destructive disasters that leave even once-prosperous survivors without any valuable assets for collateral. Finally, granting the authority only for major disasters may recognize that the SBA responds to a variety of disasters and that disasters of differing severity may warrant different credit policies.

[64] Executive Order 13632 of December 7, 2012, "Establishing the Hurricane Sandy Rebuilding Task Force," 77 *Federal Register* 74341, December 14, 2012, https://www.federalregister.gov/d/2012-30310.

[65] See recommendation 42 on p. 25 of Hurricane Sandy Task Force, *Hurricane Sandy Rebuilding Strategy: Progress Update – Spring 2014*, https://archives.hud.gov/news/2014/pr14-076-sandy-rebuilding-0614.pdf.

[66] SBA, "Disaster Assistance Loan Program; Disaster Loan Credit and Collateral Requirements," 79 *Federal Register* 22859, April 25, 2014, https://www.federalregister.gov/d/2014-09183.

[67] SBA, "Disaster Assistance Loan Program."

Second, the act increased the statutory collateral threshold for physical disaster loans (home and business) to $25,000 (from $14,000) for all disaster types, and the act allowed the SBA Administrator discretion to administratively increase the threshold for all disaster types (not just major disasters). The increased threshold and the SBA Administrator's expanded discretion were set to expire after three years, in 2018. However, they were both temporarily extended twice: through 2019 (by P.L. 115-280) and through 2022 (by the Rebuilding Small Businesses After Disasters Act, P.L. 116-70). Both temporary provisions expired on November 25, 2022.

The SBA made two administrative changes to collateral thresholds since the expiration of the temporary changes provided by the RISE After Disaster Act of 2015. First, in June 2023, the SBA amended its regulations to grant itself greater discretion regarding when to take collateral for loans above the collateral threshold. Before the change, borrowers were required to provide available collateral. After the change, borrowers are required to provide available collateral *as determined by the SBA*. The rulemaking stated that "this increased flexibility will allow SBA to tailor this collateral requirement to the disaster survivor's circumstances. For example, requiring liens on property with no liquidation value may increase the cost burden to the borrower without providing meaningful liquidated recovery for SBA in the event of a default."[68]

Second, in July 2024, the SBA exercised its statutory discretion to increase certain collateral thresholds. At that time, the SBA set the collateral thresholds for physical disaster loans (home and business) made pursuant to a major disaster and all EIDLs at $50,000 (for most loan types, up from $25,000), while the threshold for physical disaster loans made pursuant to an SBA-declared disaster is the statutory value of $14,000 (down from $25,000). The SBA stated that it expected that the change would reduce the share of disaster loans that require collateral from 46% under the previous thresholds to 31% under the new thresholds.[69]

SBA Disaster Loan Debt Collection Policy

Following a default, the SBA is required under the Debt Collection Improvement Act of 1996 (P.L. 104-134, as amended) to "maximize collections of delinquent debts owed to the Government by ensuring quick action ... and the use of all appropriate collection tools."[70] The SBA uses an escalating collection process that depends upon the length of time a disaster loan has been in default. The collection process starts with a past due notice and payment reminder calls after around one month of payment delinquency. Collection efforts then escalate over time to include due process notices, acceleration of the total amount due,[71] seizure and liquidation of collateral, reporting to credit bureaus, and referrals to the Treasury for enhanced collection efforts.[72]

Delinquency and Default

During the first 60 days following a missed payment, the SBA begins the debt collection process by sending the borrower past due notices in the mail and making automated payment reminder

[68] SBA, "Disaster Assistance Loan Program Changes to Maximum Loan Amounts and Miscellaneous Updates," 88 *Federal Register* 39335, June 16, 2023, https://www.federalregister.gov/d/2023-12779.

[69] SBA, "Disaster Assistance Loan Program Changes to Unsecured Loan Amounts and Credit Elsewhere Criteria," 89 *Federal Register* 59826, July 24, 2024, https://www.federalregister.gov/d/2024-16207.

[70] 31 U.S.C. §3701 note.

[71] Acceleration of the loan means that the full amount remaining on the loan is due immediately, regardless of the previous repayment schedule.

[72] SBA SOP 50 52 2.

phone calls. The SBA's initial goal following a missed loan payment is to return the loan to regular servicing status (that is, to get the borrower back to making regular payments as agreed upon). The SBA uses a variety of tools to do this, depending upon the borrower's situation. These include the following:

- A **deferment**, which can suspend monthly payments for a period of time in response to a temporary challenge.[73] For example, a borrower's income might be low for several months because a temporary injury prevents the borrower from working. Loan payments can resume after the borrower recovers and returns to work.
- **Severe financial hardship relief**, which can modify loan terms to assist borrowers who have experienced significant adverse events since receiving the SBA disaster loan.[74] For instance, the SBA may grant permanent or temporary changes to the loan terms, such as lower monthly payments or a lower interest rate. In addition, this relief delays the SBA's decision to move the loan into liquidation and collection.
- A **workout**, which is an agreement between the SBA and the borrower to make substantive changes to the loan that enable the borrower to repay as much of the original loan as possible while avoiding the need for actions such as foreclosure, liquidation of collateral, bankruptcy, and enhanced debt collection. Some of the possible loan changes include forbearance, changing the monthly payment amount, lowering the interest rate, or allowing the borrower to sell collateral to pay down the loan.[75] The workout process can start as late as the beginning of the collateral liquidation process. A workout is often the last chance for the SBA and the borrower to resolve the debt before debt collection and/or litigation.

Debt Collection and Charge-Off

Debt collection activity increases significantly when a loan is over 60 days past due, as shown in **Table 5**. At that time, the SBA sends the borrower and loan guarantors a "60 day" due process letter to inform them that the SBA intends, in an additional 60 days (that is, at 120 days delinquent), to send the loan to the Treasury for enhanced debt collection. The borrower has until the end of that 60-day period to pay the full amount of the loan, enter into a satisfactory installment agreement to repay the loan, or prove that the borrower is not legally liable for the debt (such as due to bankruptcy or fraud).[76] At 75 days past due, the SBA sends a demand notice, which formally accelerates the entire amount due on the loan and demands payment for the full amount. Automated payment reminder phone calls also continue through this period. The borrower has "reasonable time" following the 60-day due process notice to enter into an acceptable workout plan for the loan.[77] If the borrower and the SBA fail to reach an agreement, then the SBA will begin to liquidate collateral.

[73] SBA SOP 50 52 2, pp. 70-72.

[74] SBA SOP 50 52 2, pp. 40-44.

[75] SBA SOP 50 52 2, pp. 84-86.

[76] For due process requirements, see 13 C.F.R. §140.3.

[77] SBA SOP 50 52 2, p. 84.

Table 5. Timeline of SBA Actions Following Disaster Loan Delinquency

Days After Delinquency	SBA Actions	
1-59	The SBA seeks to get the loan back to regular repayment status through tools such as deferment, severe financial hardship relief, and workout plans.	Throughout the delinquency period before charge-off and referral to Treasury, the SBA makes automated payment reminder phone calls and mails past due notices.
60	The SBA sends the "60 day" due process letter informing the borrower that the SBA intends to refer the debt to Treasury for collection in an additional 60 days.	
75	The SBA sends a demand notice, formally accelerating (demanding full payment of) the delinquent debt.	
120+	Once the SBA has completed collateral liquidation, the loan is eligible to be charged off (removed from the SBA's books), transferred to Treasury's Cross-Servicing program and the Treasury Offset Program, and reported to credit bureaus and the federal database of defaulted borrowers; for cancelled or uncollectible debt, the SBA issues an IRS Form 1099-C (which may have tax consequences for the borrower).	

Source: Table created by CRS based on Small Business Administration (SBA), *Disaster Loan Servicing and Liquidation*, SOP 50 52 2, September 1, 2015, https://www.sba.gov/sites/default/files/files/SOP_50_52_2_1.pdf, and other SBA policies.

Notes: Dates following delinquency are approximate; specific actions may occur at different times depending upon the facts and circumstances. See the accompanying text for additional information about each action.

The SBA takes a number of additional actions once loans are 120 days past due. After this time, if the SBA has completed all debt collection actions for which expected recoveries exceed expected costs and does not anticipate additional payments, debt collection, or recoveries on the loan, it will *charge off* the remaining balance. Charge-off is an administrative accounting action by which the SBA recognizes the loss of the unpaid loan amount, for purposes of its own financial reporting. Charge-off is not loan forgiveness and it does not release the borrower or guarantors from needing to repay the loan. Instead, charge-off formally moves the loan from liquidation to a post-liquidation status that makes it eligible for additional collection tools.[78]

Following charge-off, the SBA may take several actions. For debts that have been canceled for being uncollectible (such as due to an accepted offer in compromise[79]), the SBA issues an Internal Revenue Service (IRS) Form 1099-C reporting the cancellation of debt; the canceled debt amount may be taxable income to the borrower. The SBA reports the debt to private credit reporting bureaus; having the debt on their credit record may make it harder for the borrower to obtain credit (private or government) in the future. The SBA also reports the debt to the federal Credit Alert Verification Reporting System (CAIVRS); having debt recorded in the CAIVRS generally makes a borrower ineligible for future federal loans.[80]

[78] SBA SOP 50 52 2, pp. 120-121.

[79] An *offer in compromise* is an agreement between the SBA and the borrower to settle the debt for less than the full amount owed. The SBA states that, "generally, an offer in compromise will be accepted if it reflects the [borrower's] true ability to pay, and will be rejected if the [borrower] can pay the loan in full via a lump sum payment or an installment agreement, or if acceptance of the offer would harm the integrity of the SBA disaster loan program." See SBA SOP 50 52 2, p. 106.

[80] For more about CAIVRS, see U.S. Department of Housing and Urban Development, "Credit Alert Verification Reporting System (CAIVRS)," accessed March 25, 2026, https://www.hud.gov/stat/sfh/caivrs-system.

If the remaining debt is still collectible, the SBA sends it to the Treasury's Cross-Servicing program and the Treasury Offset Program.[81] The Treasury conducts enhanced debt collection activities such as (as applicable) garnishing wages or offsetting federal payments to the borrower, including federal contractor payments, Social Security benefits, federal income tax refunds, and other payments. Borrowers remain subject to federal payment offset until the debt is repaid, the debt becomes unenforceable (such as through bankruptcy, death, or a statute of limitations), or the Treasury accepts an offer in compromise. In FY2024 (the most recent full fiscal year data available), the SBA reported recovering $126.5 million on charged-off disaster loans, mostly through Treasury efforts.[82]

Concluding Observations

The SBA disaster loan program expanded during the COVID-19 pandemic, largely due to the issuance of nearly 4 million COVID EIDLs for a total of nearly $387 billion.[83] Given this portfolio growth and the SBA's ongoing responsibilities in servicing these loans, the core underwriting and debt collection policies in the program may be of increased interest.[84] In the disaster loan program, Congress and the SBA seek to balance a "sympathetic consideration" of the needs of disaster survivors with the need to financially safeguard the program (and taxpayers) from losses.[85] Disaster loan program policies regarding credit standards, required collateral, and debt collection all contribute to this balance at different points in the loan lifecycle. Credit standards determine which borrowers can get a disaster loan and prevent lending to applicants who do not have a realistic chance of repaying the loan. Collateral policy determines the level of security of the loan if the borrower were to default on payments. Collection policy comes into play after default and liquidation of collateral; collection policy represents the federal government's last chance to be repaid, by enforcing debt collection from other sources, including wages, tax refunds, and Social Security benefits.

[81] For more about the Treasury's debt collection programs, see CRS Report RL34660, *Federal Government Debt Collection: An Overview of the Treasury Offset and Federal Payment Levy Programs*, by Gary Guenther.

[82] SBA, "Small Business Administration Loan Program Performance," data as of June 30, 2025, https://www.sba.gov/document/report-small-business-administration-loan-program-performance.

[83] The unpaid principal balance (the outstanding loan amount without interest) for the SBA disaster loan program increased from $9.6 billion at the end of FY2019 to $367.0 billion at the end of FY2022. SBA, "Small Business Administration Loan Program Performance."

[84] For example, the SBA Office of Inspector General issued an audit report on the SBA's collection efforts on delinquent COVID EIDLs in August 2025. SBA Office of Inspector General, "SBA's Collection Efforts on Delinquent COVID-19 EIDLs," Report 25-23, August 12, 2025, https://www.sba.gov/document/report-25-23-sbas-collection-efforts-delinquent-covid-19-eidls.

[85] The SBA SOPs for the disaster loan program remind employees of this need for balance several times. For example, see SOP 50 30 9, p. 96, and SOP 50 52 2, pp. 6, 7, 43, 46, and 49.

Author Information

Anthony A. Cilluffo
Analyst in Public Finance

Maria Kreiser
Senior Research Librarian

Bruce R. Lindsay
Specialist in American National Government

Acknowledgments

The authors gratefully acknowledge the contributions of the following individuals at CRS: Grant Driessen, Acting Section Research Manager; Krista Faries, Editor; Julie Lawhorn, Analyst in Economic Development Policy; Adam Levin, Analyst in Economic Development Policy; Brent Mast, Acting Coordinator of Research Planning; Maura Mullins, Acting Section Head; and Lauren Stienstra, Section Research Manager.

Disclaimer

Farm Credit System

Updated May 17, 2016

Congressional Research Service
https://crsreports.congress.gov
RS21278

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The Farm Credit System (FCS) is a nationwide financial cooperative lending to agricultural and aquatic producers, rural homeowners, and certain agriculture-related businesses and cooperatives. Established in 1916, this government-sponsored enterprise (GSE) has a statutory mandate to serve agriculture. It receives tax benefits but no federal appropriations or guarantees. FCS is the only direct lender among the GSEs. Farmer Mac, a separate GSE but regulated under the umbrella of FCS, is a secondary market for farm loans. Federal oversight by the Farm Credit Administration (FCA) provides for the safety and soundness of FCS institutions.

Current issues and legislation affecting the FCS are discussed in CRS Report RS21977, *Agricultural Credit: Institutions and Issues*.

The Farm Credit System

The Farm Credit System (FCS) was created to provide a permanent, reliable source of credit to U.S. agriculture. Before the Federal Farm Loan Act was enacted in 1916, credit was often unavailable or unaffordable in rural areas. Many lenders avoided farm loans due to the inherent risks of agriculture. Statutory authority is in the Farm Credit Act of 1971, as amended (12 U.S.C. 2001 *et seq.*). Comprehensive changes were enacted in the Agricultural Credit Act of 1987.

The FCS is authorized by statute to lend to farmers, ranchers, and harvesters of aquatic products. Loans may also be made to finance the processing and marketing activities of these borrowers; for home ownership in rural areas; certain farm- or ranch-related businesses; and agricultural, aquatic, and public utility cooperatives.

FCS is a commercial for-profit lender and is *not* a lender of last resort.[1] Borrowers must meet creditworthiness requirements similar to those of a commercial lender. FCS has "young, beginning, and small" (YBS) farmer lending programs, but they do not have statutory targets or mandates.

The FCS holds nearly 41% of the farm sector's total debt (about the same as the 42% share by commercial banks) and has the largest share of farm real estate loans (46%).[2] As of March 31, 2016, FCS had $238 billion in loans outstanding, of which about 46% was in long-term agricultural real estate loans, 19% in short- and intermediate-term agricultural loans, 15% in loans to agribusinesses, 8% in energy and water/waste water loans, 2% in export financing loans and leases, 3% in rural home loans, and 3% in communications loans (**Figure 4**).[3]

Government-Sponsored Enterprise (GSE)

As a GSE, FCS is a privately owned, federally chartered cooperative designed to provide credit nationwide. It is limited to serving agriculture and related businesses and homeowners in rural areas. Each GSE is given certain benefits, such as implicit federal guarantees or tax exemptions, presumably to overcome barriers faced by purely private markets.[4] FCS is the only direct lender among the GSEs. Other GSEs, such as Fannie Mae, are secondary markets. FCS is not a government agency, and it is not explicitly guaranteed by the U.S. government.[5]

The tax benefits for FCS include an exemption from federal, state, municipal, and local taxation on the profits earned by the real estate side of FCS (12 U.S.C. 2098). Income earned by the non-real-estate side of FCS is subject to taxation. The exemption originated in the 1916 act. Commercial bankers estimate that the annual value of these tax benefits amounted to over $1 billion in 2011.[6] For investors who buy FCS bonds on Wall Street, the interest earned is exempt

[1] The Farm Service Agency (FSA) is a lender of last resort for borrowers who are unable to get a loan from another lender. For more general background, see CRS Report RS21977, *Agricultural Credit: Institutions and Issues*.

[2] See CRS Report RS21977, *Agricultural Credit: Institutions and Issues*.

[3] Federal Farm Credit Banks Funding Corporation, Quarterly Information Statement, March 31, 2016, http://www.farmcreditfunding.com/ffcb_live/financialInformation.html?tab=statements.

[4] There are five GSEs: Federal National Mortgage Association (Fannie Mae), Federal Home Loan Mortgage Corporation (Freddie Mac), Federal Home Loan Bank System, Federal Agricultural Mortgage Corporation (Farmer Mac), and FCS. For more on GSEs, see CRS Report RL30533, *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics*.

[5] Because of the significant role of GSEs in the U.S. economy, many investors believe that the federal government will not allow a GSE to fail. Thus, an implicit, albeit not statutory, guarantee exists.

[6] *Farm Credit Watch*, February 2012.

from state, municipal, and local taxes. This makes FCS bonds more attractive to the investing public and helps assure a plentiful supply of funds for loans. Commercial bankers say that the tax benefits let FCS offer lower interest rates to borrowers and thus give FCS an operating advantage, since they compete in the same retail lending market.

Cooperative Business Organization

FCS associations are owned by the borrowers who purchase stock, which is required as part of their loans (the smaller of $1,000 or 2% of the loan amount). FCS stockholders elect the boards of directors for banks and associations. Each has one vote, regardless of the loan size. Most directors are members, but federal law requires at least one from outside.

If an association is profitable, the directors may choose to retain the profits or distribute some of it through dividends or *patronage refunds* that are proportional to the size of the loan. Patronage refunds can effectively reduce the cost of borrowing.

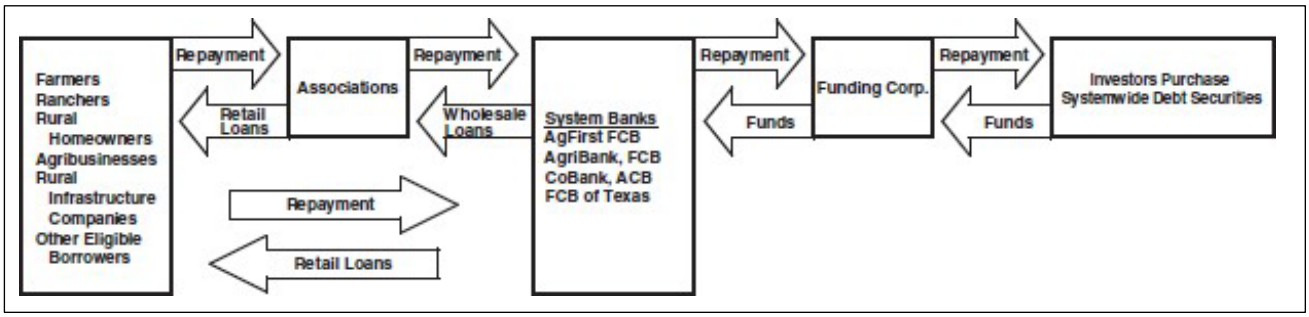
Funded with Bonds and Stock and Insured

With the exception of seed money that was repaid by the 1950s and a temporary U.S. Treasury line of credit in the 1980s,[7] FCS operates without any direct federal appropriations. FCS banks and associations do not take deposits like commercial banks.

Instead, the **Federal Farm Credit Banks Funding Corporation** uses capital markets to sell FCS bonds and notes.[8] These debts become the joint and several liabilities of all FCS banks. The funding corporation allocates funding to the banks, which provide funds to associations, which lend to borrowers. Profits from loans repay bondholders (**Figure 1**).

FCS also raises capital through two other methods. Borrowers are required to buy stock (the lesser of $1,000 or 2% of the loan amount) and become cooperative members. FCS also retains profits that are not returned as patronage to borrowers.

Figure 1. Flow of Funds Through the FCS Between Bondholders and Borrowers



Source: Farm Credit System, 2015 Annual Information Statement.

Besides relying on the capital that the FCS has built, obligations of the FCS are further insured by the **Farm Credit System Insurance Corporation**, which was established by statute in 1988 to ensure timely payment of principal and interest on FCS debt securities. Annual premiums are paid

[7] The Financial Assistance Corporation (FAC) borrowed $1.26 billion from Treasury during the farm financial crisis of the 1980s. In 2005, these bonds were repaid with interest. The FAC was dissolved in December 2006.

[8] The Funding Corporation is a central source for FCS financial statements at http://www.farmcredit-ffcb.com.

by each bank through an assessment based on loan volume until the secure base amount of 2% of total outstanding loans is reached.

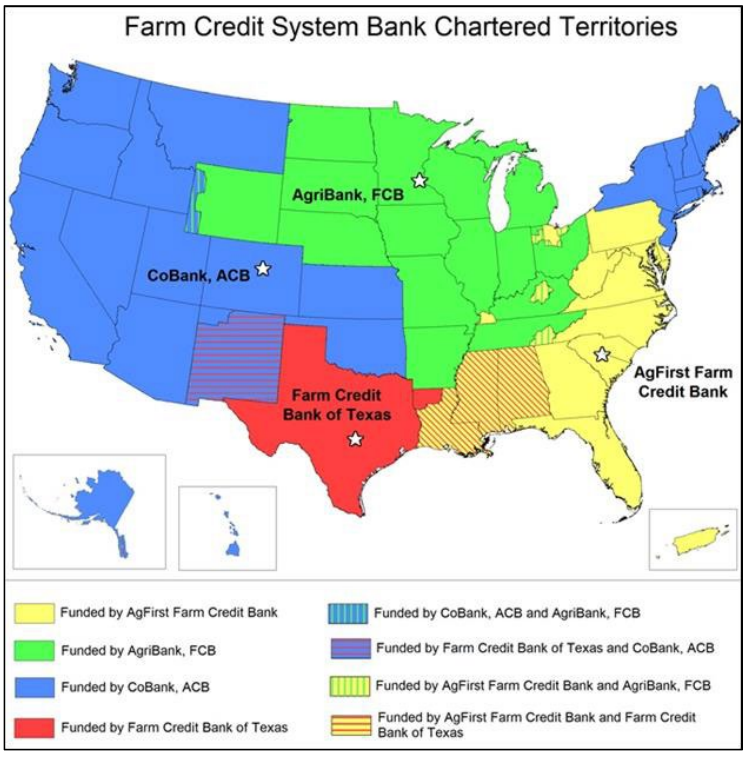
National System of Banks and Associations

FCS is composed of four regional banks (**Figure 2**) that provide funds and support services to 74 smaller Agricultural Credit Associations (ACAs), Federal Land Credit Associations (FLCAs), and Production Credit Associations (PCAs). These associations (**Figure 3**), in turn, provide loans to eligible borrowers. The most common operating structure (due to favorable tax and regulatory rules) is a "parent ACA" with FLCA and PCA subsidiaries. There are 72 ACAs and two FLCAs.[9]

In addition to its charter as one of the regional banks, CoBank has a nationwide charter to finance farmer-owned cooperatives and rural utilities. It finances agricultural exports and provides international services for farmer-owned cooperatives through three international offices.

The number of banks and associations has been declining for decades through mergers and reorganizations. This consolidation has continued in recent decades through the "parent ACA" structure. In the mid-1940s, there were over 2,000 lending associations. There were nearly 900 in 1983, fewer than 400 by 1987, 200 in 1998, 95 in 2006, and 80 in 2015. The system operated with 12 districts into the 1980s, 8 districts in 1998, 5 districts in 2004, and 4 regional banks since 2012.

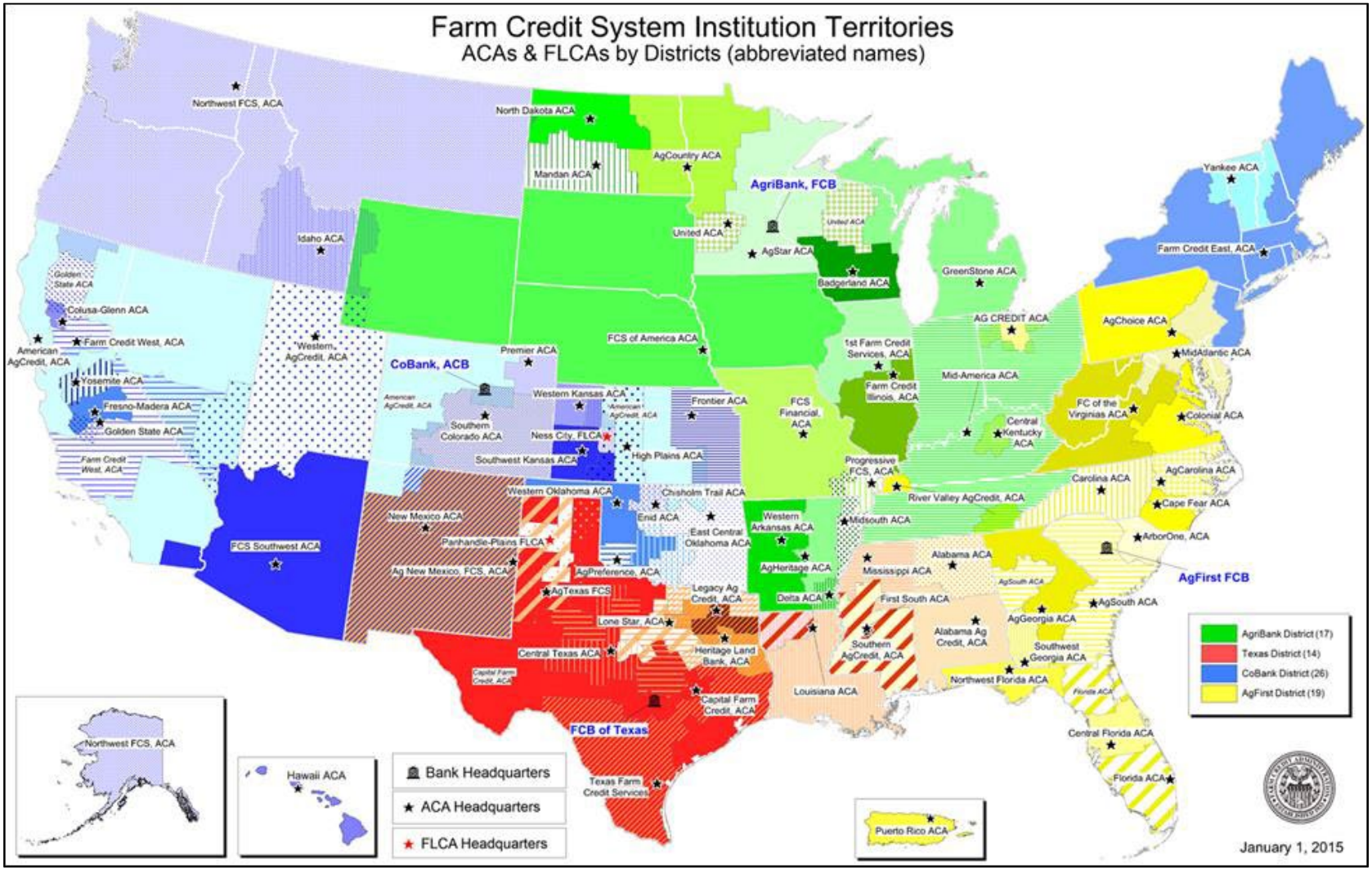
Figure 2. Farm Credit System as of January 1, 2016



Source: Farm Credit Administration, at http://www.fca.gov/info/directory.html.

[9] The Farm Credit Administration maintains a directory of FCS institutions at http://www.fca.gov/info/directory.html.

Figure 3. Farm Credit System Associations That Deliver Loans to Borrowers



Source: Farm Credit Administration, http://www.fca.gov/info/directory.html.

Twenty years ago, the typical FCS association covered several counties and specialized in either land or farm production loans. Today, the typical FCS association covers a much larger region, delivers a wide range of farm and rural credit programs and services, and has an extensive loan portfolio. FCS may benefit when consolidation creates more diversified portfolios. Customers may benefit if greater institutional efficiency is passed along through lower interest rates. However, consolidation may weaken the original cooperative concept of local borrower control.

Each association within FCS has a specific "charter territory." If an association wants to lend outside its charter territory, it must first obtain approval from the other territory's association. Charter territories help ensure that borrowers are served locally and maintain local control of the association. Charter territories and any changes must be approved by FCA.

Types of Loans and Borrowers

The FCS provides three types of loans to farm producers: (1) operating loans for the short-term financing of consumables such as feed, seed, fertilizer, or fuel; (2) installment loans for intermediate-term financing of durables such as equipment or breeding livestock; and (3) real estate loans for long-term financing (up to 40 years) of land, buildings, and homes.

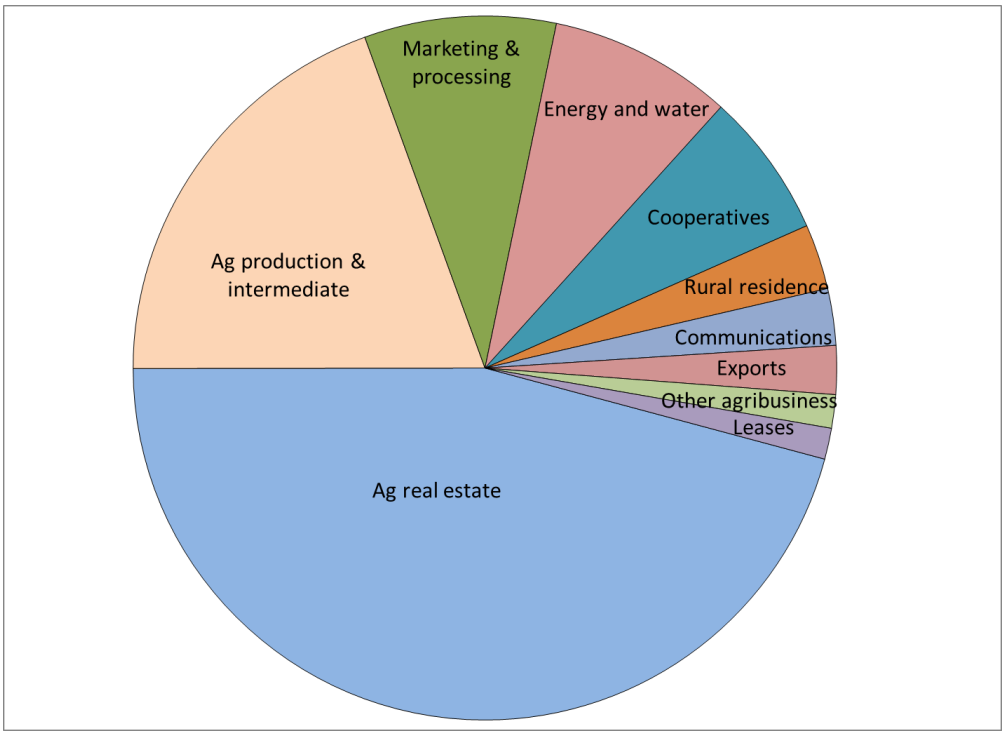
The FCS has a statutory mandate to serve agriculture, certain agribusinesses, and rural homeowners (e.g., 12 U.S.C. 2019 and 2075). Borrowers must meet eligibility and creditworthiness requirements. Types of eligible borrowers and the scope of their financing can be grouped into the following categories (e.g., 12 U.S.C. 2017, 2075, and 2129):

- **Full-time farmers.** For individuals with over 50% of their assets and income from agriculture, FCS can lend for all agricultural, family, and non-agricultural needs (including vehicles, education, home improvements, and living expenses).
- **Part-time farmers.** For individuals who own farmland or produce agricultural products but earn less than 50% of their income from agriculture, FCS can lend for all agricultural and family needs. Non-agricultural lending is limited.
- **Farming-related businesses.** FCS can lend to businesses that *process* or *market* farm, ranch, or aquatic products if more than 50% of the business is owned by farmers who provide at least some of the "throughput." FCS can also lend to businesses that *provide services* to farmers and ranchers, such as crop spraying and cotton ginning. The extent of financing is based on the amount of the business's farm-related income.
- **Rural homeowners.** FCS can lend for the purchase, construction, improvement, or refinancing of single-family dwellings in rural areas (2,500 population limit).
- **Farmer-owned cooperatives and certain rural utilities** (electric and telecom).

Figure 4 illustrates FCS's portfolio of loans outstanding ($238 billion as of March 31, 2016). About 65% of the loan portfolio is in the primary categories of farm real estate and operating loans.

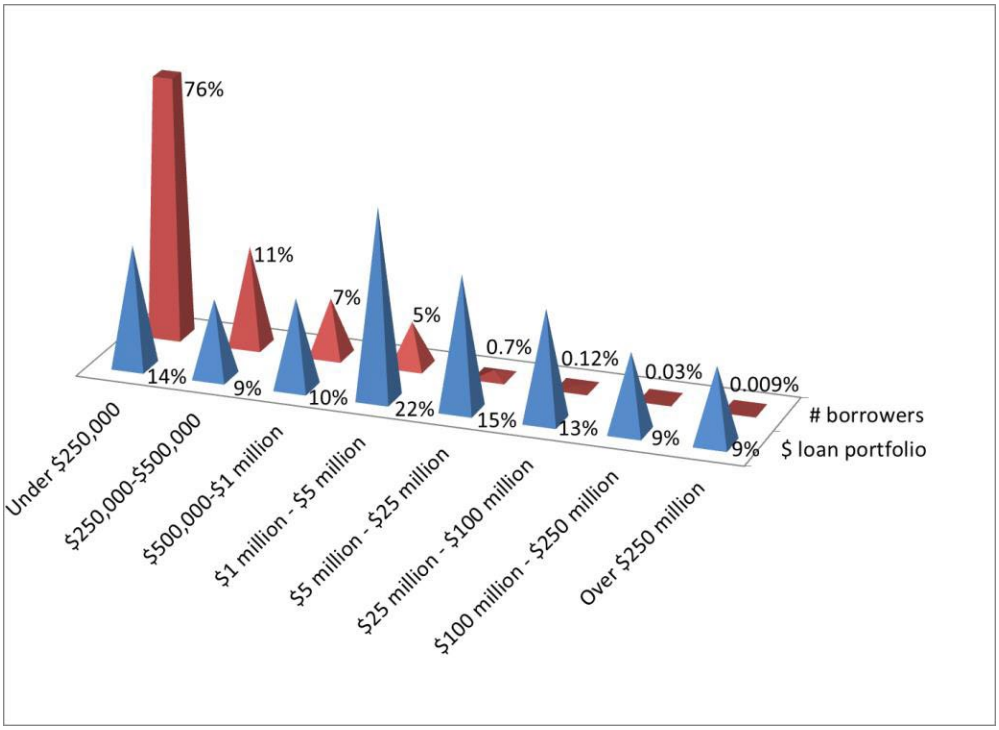
Figure 5 presents the loan portfolio by size of loan and the number of borrowers in each size category. About 74% of borrowers (402,000 out of 527,000) have loans under $250,000 in size and account for 14% of the loan portfolio. At the other extreme, 49 borrowers (0.009% of 527,000) have loans over $250 million and account for 9% of the loan portfolio.

Figure 4. Farm Credit System Loan Portfolio by Type of Loan, 2016



Source: CRS, based on Farm Credit System, Quarterly Information Statement, March 31, 2016.

Figure 5. Farm Credit System Loan Portfolio by Size of Loan, 2015



Source: CRS, based on Farm Credit System, 2015 Annual Information Statement, Dec. 31, 2015.

Federal Regulation

Congressional Oversight

Congressional oversight of FCS is provided by the House and Senate Agriculture Committees, which have primary jurisdiction for the FCS statutes.

The most recent congressional hearings on agricultural credit were in the House on December 2, 2015 (with witnesses from the FCA),[10] and in the Senate on June 13, 2006 (on agricultural credit but not specifically the FCS).[11] The Senate Agriculture Committee also holds hearings on nominees for the Farm Credit Administration board of directors, most recently in March 2015.[12]

Farm Credit Administration (FCA)

FCA is an independent agency and the federal regulator responsible for examining and ensuring the safety and soundness of all FCS institutions (12 U.S.C. 2241 *et seq*.; 12 C.F.R. 600 *et seq*.).

FCA is directed by a three-member board nominated by the President and confirmed by the Senate (**Table 1**). Board members serve six-year terms and may not be reappointed after serving a full term or more than three years of a previous member's term. The President designates one member as chairman, who serves until the end of that member's term. Members may continue to serve on the board until their replacements are confirmed.

FCA's operating expenses are paid through assessments on FCS banks and associations. Even though FCA does not receive an appropriation from Congress, the annual agriculture appropriations act places a limit on FCA's administrative expenses ($65.6 million in FY2016).

Table 1. Farm Credit Administration Board of Directors

Name	Senate Confirmation and Comments	Term Expires
Kenneth A. Spearman, Chairman	Confirmed on 10/8/2009 to complete the term of Dallas P. Tonsager that was to expire 5/21/2010. Reappointed to full term. Appointed chairman of the board and CEO on March 13, 2015.	5/21/2016
Jeffrey S. Hall	Confirmed on March 9, 2015.	10/13/2018
Dallas P. Tonsager	Confirmed on March 9, 2015. Previously an FCA board member for a partial term from 2004 to 2009.	5/21/2020

Source: CRS.

[10] House Committee on Agriculture, "To Review the Farm Credit System," public hearing on December 2, 2015, http://agriculture.house.gov/calendar/eventsingle.aspx?EventID=3032.

[11] Senate Committee on Agriculture, Nutrition and Forestry, "Review of USDA Farm Loan Programs," hearing on June 13, 2006, http://www.ag.senate.gov/hearings/review-usda-farm-loan-programs.

[12] Senate Committee on Agriculture, Nutrition and Forestry, "Nominations," http://www.ag.senate.gov/nominations.

Issues for Congress

Competition and "Similar Entity Lending"

Competition between the FCS and commercial banks is an ongoing source of contention related to congressional oversight and statutory jurisdiction. The FCS is unique among the GSEs because it is a retail lender making loans directly to farmers and thus is in direct competition with commercial banks. Because of this direct competition for creditworthy borrowers, the FCS and commercial banks often have an adversarial relationship over policy.

Commercial banks assert unfair competition from the FCS for borrowers because of tax advantages that can lower the relative cost of funds for the FCS.[13] They often call for increased congressional oversight. The FCS counters by citing its statutory mandate (and limitations) to serve agricultural borrowers in good times and bad times.[14]

Recently, the assertion of unfair competition and inappropriate lending has been leveled over the characteristics of some borrowers that have obtained FCS loans and/or the purposes of those loans.[15] The policy-related issue is the purpose and extent of the statutory authority for "similar entity lending" that certain FCS banks have used to participate (i.e., have a partial interest, or to buy part of a loan from another bank) in loans to borrowers that would otherwise be ineligible for direct FCS loans.

The authority to make "similar entity loans" was added to the Farm Credit Act in 1994 (P.L. 103-376, Section 5). It allows the FCS to participate in loans that are originated by a commercial bank to borrowers that are expressly *not* eligible for FCS loans but for purposes that are "functionally similar" to activities that are conducted by FCS-eligible borrowers (12 U.S.C. 2206a; 12 C.F.R. 613.3300, 62 *Federal Register* 4444, January 30, 1997). The provision is meant to allow greater diversification in the FCS loan portfolio for risk management along with traditional means of diversification (such as geographic breadth) and lending to a range of commodity sectors. "Similar entity loans" cannot exceed 15% of the FCS entity's total loan volume and must be less than 50% of the individual loan.

Commercial banking advocates charge that many of the similar entity loans fail a perception test of meeting the original statutory intent that FCS makes credit available to farmers and rural communities and are often inappropriately large or risky. FCS advocates counter that the loans are legal under the statute, follow the intent of achieving diversification, and help commercial banks by jointly cooperating through loan participations.

Several Members at a House Agriculture Committee hearing in December 2015 raised questions about the appropriateness and perception of some similar entity loans, despite statements about

[13] See, for example, American Bankers Association, letter to House and Senate Agriculture Committees, February 2, 2015, http://www.aba.com/Advocacy/LetterstoCongress/Documents/LetterSenateAgCommreFCS-Oversight020215.pdf.

[14] See, for example, Farm Credit Council, letter to House and Senate Agriculture Committees, February 5, 2015, http://www.fccouncil.com/files/FCC_Letters_in_Response_to_ABA_5Feb2015.pdf.

[15] For example, the FCS participation in a loan to Verizon is highlighted in the *Denver Post*, "Group Challenges CoBank's Financing of Verizon-Vodafone Deal," October 23, 2013, at http://www.denverpost.com/breakingnews/ci_24365106/group-challenges-cobanks-financing-verizon-vodafone-deal.

the legality of such loans.[16] In response to the hearing,[17] FCA issued a "bookletter"[18] in March 2016 that provided further guidance and reporting requirements for FCS associations to guard against reputation risk from similar entity lending.[19]

Recent Farm Bills

The most recent statutory changes to the Farm Credit Act have been in omnibus farm bills, and those changes have been relatively minor in terms of the scope of FCS lending or the structure of the institution. For example, the 2014 farm bill (P.L. 113-79) established the intent that compensation disclosure of FCS executives rests with FCS boards of directors rather than elsewhere, such as with shareholders.[20] The previous farm bill in 2008 (P.L. 110-246) allowed the Federal Agricultural Mortgage Company (Farmer Mac, see below) to participate in rural utility loans and made technical changes to the premiums paid by FCS banks to the FCS Insurance Corporation, but it did not expand the scope of FCS authority as some advocates had hoped.[21]

Farmer Mac—Another Farm Credit Act Institution

The Federal Agricultural Mortgage Company (Farmer Mac) was established in the Agricultural Credit Act of 1987 as a secondary market for agricultural loans. It purchases and pools qualified loans and may sell them to investors as securities or hold them in its own portfolio.

Although Farmer Mac is statutorily part of the Farm Credit Act and is regulated by FCA, it has no liability for the debt of any other FCS institution, and the other FCS institutions have no liability for Farmer Mac debt. It is considered a separate GSE.

Farmer Mac is an investor-owned corporation, not a member-owned cooperative. Voting stock may be owned by banks, insurance companies, and FCS institutions. Nonvoting stock may be owned by any investor. Its board of directors has members from the FCS, commercial banks, and the public at large.

Farmer Mac operates two programs: Farmer Mac I (loans not guaranteed by the U.S. Department of Agriculture [USDA]) and Farmer Mac II (USDA-guaranteed loans).

- A majority of **Farmer Mac I** volume comes from the sale of "long-term standby purchase agreements." Farmer Mac promises to purchase specific agricultural mortgages, thus guaranteeing the loans against default risk while the participating lender retains interest rate risk.

[16] House Committee on Agriculture, "Transcript of Hearing to Review the Farm Credit System," December 2, 2015, http://agriculture.house.gov/uploadedfiles/12.2.15_hearing_transcript.pdf.

[17] Jeffrey S. Hall, FCA board member, "Statement in Support of Bookletter 67," March 10, 2016, http://www.fca.gov/Download/Statements/hall10march2016_2.pdf.

[18] Bookletters are documents issued by an official that communicate FCA's legal interpretations and its position on specific issues.

[19] FCA, Bookletter BL-67, "Lending to Similar Entities," March 10, 2016, http://ww3.fca.gov/readingrm/Handbook/FCA%20Bookletters/BL-067.docx?Web=1.

[20] In 2012, FCA had published a rule that provided for advisory votes by shareholders on senior officer compensation (12 C.F.R. 611.360; 77 *Federal Register* 60596, October 3, 2012). That rule was withdrawn following the provision in the 2014 farm bill (Section 5404 of P.L. 113-79; 79 *Federal Register* 17856, March 31, 2014).

[21] Although the House Agriculture Committee-reported version of the farm bill in 2007 contained provisions to expand the scope of the FCS loans, those provisions were removed by a floor amendment from leaders of the House Financial Services Committee (H.Amdt. 702 to H.R. 2419).

- Under **Farmer Mac II**, the company purchases the portion of individual loans that are guaranteed by USDA. On these purchases, Farmer Mac accepts the interest rate risk but carries no default risk.

Author Information

Jim Monke
Specialist in Agricultural Policy

Disclaimer