

Word Count: 4,344

SUPREME COURT
STATE OF COLORADO

2 East 14th Avenue
Denver, CO 80203

On Certiorari to the Colorado Court of
Appeals

Court of Appeals Case No. 10CA0587

THE PEOPLE OF THE STATE OF
COLORADO,

Plaintiff-Appellee,

v.

EDUARDO PEREZ,

Defendant-Appellant.

CYNTHIA H. COFFMAN, Attorney General

KEVIN E. MCREYNOLDS, Assistant
Attorney General*

Ralph L. Carr Colorado Judicial Center

1300 Broadway, 9th Floor

Denver, Colorado 80203

Telephone: 720-508-6485

E-Mail: kevin.mcreynolds@state.co.us

Registration Number: 40978

*Counsel of Record

DATE FILED: June 4, 2015 5:05 PM
FILING ID: DB0B2FE818C36
CASE NUMBER: 2013SC465

▲ COURT USE ONLY ▲

Case No. 13SC465

PEOPLE'S REPLY BRIEF

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with all requirements of C.A.R. 28 and C.A.R. 32, including all formatting requirements set forth in these rules. Specifically, the undersigned certifies that:

The brief complies with C.A.R. 28(g).

It contains less than 5,700 words.

The brief complies with C.A.R. 28(k).

It contains, under a separate heading, a concise statement of the applicable standard of appellate review and a citation to where the issue was raised and ruled on.

/s/ Kevin E. McReynolds

TABLE OF CONTENTS

	PAGE
ISSUES ON WHICH CERTIORARI WAS GRANTED	1
I. The legislature intended to criminalize conduct – not merely to enhance the penalty for a limited group of particularly culpable criminal impersonators.	1
A. The statutory scheme and mens rea amendments rebut the statutory presumption Defendant relies upon.	4
B. The legislative context and drafter’s statements belie Defendant’s strained construction.	12
II. There was a logical connection between the Defendant’s repeated use of the victim’s Social Security number and the jury’s conclusion that he knew it belonged to a real person.	19
CONCLUSION	25

TABLE OF AUTHORITIES

	PAGE
CASES	
<i>Clark v. People</i> , 232 P.3d 1287 (Colo. 2010)	19, 20
<i>Copeland v. People</i> , 2 P.3d 1283 (Colo. 2000)	10
<i>Elliot Coal Mining Co. v. Dir. Office of Workers' Comp. Programs</i> , 17 F.3d 616 (3d Cir. 1994).....	4
<i>Heydon's Case</i> , 76 Eng. Rep. 637 (Ex. 1584).....	4, 16
<i>Jefferson Cnty. Bd. of Equalization v. Gerganoff</i> , 241 P.3d 932 (Colo. 2010).....	2
<i>People v. Bennett</i> , 183 Colo. 125, 515 P.2d 466 (1973)	19
<i>People v. Campos</i> , 2015 COA 47	1
<i>People v. Cross</i> , 127 P.3d 71 (Colo. 2006).....	passim
<i>People v. DeWitt</i> , 275 P.3d 728 (Colo. App. 2011).....	4, 5
<i>People v. Hernandez</i> , 250 P.3d 568 (Colo. 2011)	1, 12
<i>People v. Iversen</i> , 2013 COA 40.....	5
<i>People v. Perez</i> , 2013 COA 65.....	6
<i>Spahmer v. Gullette</i> , 113 P.3d 158 (Colo. 2005)	13
<i>Specialty Restaurant Corp. v. Nelson</i> , 231 P.3d 393 (Colo. 2010)	9
STATUTES	
§18-1-102, C.R.S. (2014)	2
§18-1-503(4), C.R.S. (2014).....	4, 5, 6
§18-5-113, C.R.S. (2012)	2, 9
§18-5-901, C.R.S. (2012)	8
§18-5-902, C.R.S. (2012)	passim
§2-4-201, C.R.S. (2014)	2

TABLE OF AUTHORITIES

	PAGE
§2-4-203, C.R.S. (2014)	13
§2-4-212, C.R.S. (2014)	1
OTHER AUTHORITIES	
HB 06-1326, House Judiciary Committee (2/23/06)	13, 14
HB 06-1326, House Second Reading (4/11/06).....	14
HB 06-1326, Senate Judiciary Committee (4/24/06)	13, 14
HB 06-1326, Senate Second Reading (5/2/06).....	15
HB-1326, Digest of Bills	3
<i>IRS Says Identity Thieves Accessed Tax Transcripts for More Than 100,000 Taxpayers</i> , Forbes, May 26, 2015.....	15
Jacob Scott, <i>Codified Cannons and the Common Law of Interpretation</i> , 98 Geo. L.J. 341 (Jan. 2010)	18
Kristin Finklea, <i>Identity Theft: Trends and Issues</i> (Congressional Research Service 2014)	15, 22
SB 09-093.....	10
SSA, Social Security Number Allocations	21, 22
SSA, Social Security Number Randomization.....	21
SSA, Social Security Testimony Before Congress (Feb 16, 2006)	22

ISSUES ON WHICH CERTIORARI WAS GRANTED

Whether the court of appeals erred in concluding Colorado's identity theft statute, section 18-5-902, C.R.S. (2012), requires proof that the offender knew the information he exploited belonged to a real person, and if so, whether no rational juror could reasonably infer that an offender knew the Social Security number he used over a five-year period belonged to a real person.¹

I. The legislature intended to criminalize conduct – not merely to enhance the penalty for a limited group of particularly culpable criminal impersonators.

The Court's "fundamental responsibility" [in this case] is to determine and give effect to the General Assembly's purpose and intent in enacting" Colorado's identity theft statute. *People v. Hernandez*, 250 P.3d 568, 570-71 (Colo. 2011); *People v. Cross*, 127 P.3d 71, 73 (Colo. 2006); *see also* §2-4-212, C.R.S. (2014) ("**Liberal construction.** All

¹ People's Reply Brief focuses on the issues before this Court. To the extent Defendant claims this Court erred by granting certiorari, the People disagree because: (1) the court of appeals *sua sponte* interpreted the identity theft statute and dismissing this portion of the certiorari question will not resolve this case; (2) Defendant's alternative "thing of value" argument was recently rejected in *People v. Campos*, 2015 COA 47; and (3) these issues are also before this Court in the parallel case *People v. Molina*, 14SC498.

general provisions, terms, phrases, and expressions used in any statute, shall be liberally construed, in order that the true intent and meaning of the general assembly may be fully carried out.”).

This task requires the Court to harmonize the statutory provisions to effectuate the just and reasonable differentiation between criminal offenses. *See Jefferson Cnty. Bd. of Equalization v. Gerganoff*, 241 P.3d 932, 935 (Colo. 2010) (“The language at issue must be read in the context of the statute as a whole and the context of the entire statutory scheme”); §2-4-201, C.R.S. (2014) (statutes are presumed to be effective, feasible to execute, and to produce a just result that favors public interests over private ones); §18-1-102(c), C.R.S. (2014) (the criminal code must be construed “[t]o differentiate on reasonable grounds between serious and minor offenses . . .”).

Here, the parties disagree on what the General Assembly intended to criminalize through section 18-5-902 and the differentiation of this new offense from the preexisting criminal impersonation statute, section 18-5-113.

The People contend the General Assembly enacted section 18-5-902 to recognize and combat a “new crime” that was harming its citizens – the knowing use of victims’ personal information for offenders’ own purposes (*see* OB pp. 11-18). *See also* HB-1326, Digest of Bills (listing the original enactment of section 18-5-902 as “Creat[ing] the following *new* crimes: Identity theft”) (emphasis added). This statute created a more serious offense where the exploited information belonged to a real person whereas criminal impersonation applied to those cases involving the use of false or fictitious information, where no real people or entities suffered harm (*see* OB pp. 5, 13).

By contrast, Defendant insists the legislature defined “identity theft” as a nothing more than a sentence enhancer for a narrow set of criminal impersonators (*see* AB pp. 15-24). In Defendant’s view, criminal impersonation applies to offenders’ use of both fictitious identifying information and that “of another” real person; limiting section 18-5-902 to those offenders who specifically knew they were exploiting real victim information (*see id.* pp. 25-26).

Defendant is wrong. This narrow and impractical construction contravenes the statutory scheme, the General Assembly’s intent, and the “mischief” it sought to address through section 18-5-902.²

A. The statutory scheme and mens rea amendments rebut the statutory presumption Defendant relies upon.

Mechanically, the parties opposing interpretations of section 18-5-902 turn on whether the mens rea of this statute “speak[s] to the conduct, or to the circumstances, or to the result, or to any combination thereof, but not necessarily to all three” (OB p. 7) (quoting *Cross*, 127 P.3d at 74). A mental state is presumed to apply to every element of the offense, unless the General Assembly intended it apply to only some elements. *See id.*; §18-1-503(4), C.R.S. (2014); *see People v. DeWitt*, 275 P.3d 728, 735 (Colo. App. 2011).

² As discussed herein, the People’s position is supported by the original canon of statutory construction: the “mischief rule” from *Heydon’s Case*. “That canon of construction directs a court to look to the ‘mischief and defect’ that the statute was intended to cure.” *Elliot Coal Mining Co. v. Dir. Office of Workers’ Comp. Programs*, 17 F.3d 616, 631 (3d Cir. 1994) (quoting *Heydon’s Case*, 76 Eng. Rep. 637 (Ex. 1584)).

As this Court recognized, “[u]nder this rule and its exception, we must carefully consider whether the legislature intended that the . . . culpable mental state applies to only certain elements” and must “avoid interpreting a statute that defeats legislative intent” by, among other things, failing to read the statutory language “in harmony with the overall statutory design.” *Cross*, 127 P.3d at 74-77 (finding the mens rea only applied to some elements of harassment based on statutory history, related provisions and accompanying declaration of policy); see *DeWitt*, 275 P.3d at 735 (finding the mens rea only applied to some elements of POWPO based on the language and purpose of the POWPO statute); see also *People v. Iversen*, 2013 COA 40 ¶¶21-24 (finding the presumption in section 18-1-503(4) inapplicable where it would thwart the legislature’s intent to obtain a just and reasonable result by excluding contraband from detention facilities). In other words, courts are not required to view the statutory text in isolation when determining whether the legislature intended the mens rea to apply to only certain elements.³

³ Though the People disagree with its ultimate conclusion, the court of

Defendant ignores this broader directive and instead argues variations of a single point – this statutory presumption is conclusive, and therefore, the knowingly mens rea in the identity theft statute applies to both the conduct (use of information/devices) and circumstance/result (this information was “of another” real person) (*see* AB pp. 15-25, 26-27).⁴ To avoid the illogic, absurdity and impracticality of this construction (which effectively legalizes the use of personal information “of another” absent this presumptive intent), Defendant claims the legislature intended the amended criminal impersonation statute to address such cases (*see* AB pp. 25-26) (discussing the 2011 amendment to section 18-5-113).

Defendant is wrong.

appeals similarly consulted extrinsic sources (legislative history and judicial interpretations) in finding the presumption in section 18-1-503(4) applied to the identity theft statute. *See People v. Perez*, 2013 COA 65 ¶¶17-22.

⁴ Defendant also chides the People for failing to “cite to or discuss” section 18-503(4) in the Opening Brief (AB p. 18). This is inaccurate. The People cited and discussed this rebuttable statutory presumption and cases rejecting this presumption (*see* OB pp. 7-8, 14-15).

Instead of rewriting the criminal impersonation statute to accommodate Defendant’s strained interpretation, this Court should instead recognize the legislature intended the mens rea for identity theft to apply to the conduct element (*see* OB pp. 5, 9-15). Thus, the General Assembly created a harmonious statutory scheme by reasonably differentiating these offenses based on the *existence* statutorily defined circumstance – the information used was “of another” natural person (*see id.*).

The text of these complementary statutes illustrates this legislative intent and the problems with Defendant’s efforts to wedge the “knowingly” mens rea into every element of identity theft. Section 18-5-902 provides in applicable part:

- (1) A person commits identity theft if he or she:
 - (a) Knowingly uses the *personal identifying information*, financial information, or financial device *of another* without permission or lawful authority with the intent to obtain cash, credit, property, services, or any other thing of value or to make a financial payment . . .

§18-5-902 (1)(a), C.R.S. (2012) (emphasis added). The legislature specifically defined the key terms “personal identifying information” and “of another” when it first enacted this crime. See §18-5-901(13), (11), C.R.S. (2012) (e.g. subsection (11) defines “of another” as meaning “that of a natural person, living or dead, or a business entity . . .”). Thus, the identity theft statute is designed to address an offender’s use of real personal identifying information (*i.e.* where there is a victim).

The parallel criminal impersonation statute does not directly address the use of a natural person’s information and instead provides:

- (1) A person commits criminal impersonation if he or she knowingly:
 - (b) Assumes a false or fictitious identity or capacity, legal or otherwise, and in such identity or capacity he or she:
 - (II) Performs any other act with intent to unlawfully gain a benefit for himself, herself or another or to injure or defraud another.
- (3) For the purposes of subsection (1) of this section, using false or fictitious *personal identifying information, as defined in section 18-5-901(13)*, shall constitute the assumption of a false or fictitious identity or capacity.

§18-5-113 (1)(b)(II), (3), C.R.S. (2012) (emphasis added). While Defendant seizes on the 2011 addition of subsection (3) and the cross-reference to offender’s use of “personal identifying information”, he ignores the much more important omission: the legislature did not add the statutorily defined term “of another” to target the use of a real victim’s information (*compare id. with* AB pp. 25-26).

This is critical to understanding how the General Assembly intended to address these related fraud offenses through its statutory scheme. Had the legislature intended the amended criminal impersonation statute to broadly address any use of personal identifying information, including that “of another” natural person, it could have cross-referenced this statutorily-defined term. It did not and this Court should respect this legislative choice, rather than assume the “of another” definition applies to criminal impersonation to avoid the gap created by Defendant’s proffered construction of identity theft. *See Specialty Restaurant Corp. v. Nelson*, 231 P.3d 393, 397 (Colo. 2010) (courts should not “construe a statute in a manner that assumes the General Assembly made an omission; rather the General Assembly’s

failure to include particular language is a statement of legislative intent”); *Cross*, 127 P.3d at 73.

The legislature’s 2009 amendment to section 18-5-902 also undermines Defendant’s presumption that the legislature intended the “knowingly” mens rea to apply to every element. As initially enacted, the new crime of identity theft included a single “knowingly” mens rea provision. Thus, under Defendant’s view, the General Assembly intended that mens rea to apply to every element.

But the legislature rejected this presumptive construction in 2009, by inserting an “intent” mens rea provision that required proof the offender “knowingly uses the personal identifying information . . . of another without permission or lawful authority **with the intent** to obtain cash, credit, property, services or any other thing of value . . .” See SB 09-093 at 1 (emphasis added). This amendment provided that different elements of section 18-5-902(1)(a) have differing mens rea requirements: the legislature did not intend the “knowingly” mens rea to apply to the offender’s purposes in exploiting victim information. See *Copeland v. People*, 2 P.3d 1283, 1286 (Colo. 2000) (“Elements of a

particular offense may have differing mens rea requirements”). This in turn creates an ambiguity as to how this amendment changed the original structure of this statute by either: (1) overriding the “knowingly” mens rea that the General Assembly originally intended apply to every element, or (2) inserting a new “intent” mens rea requirement for an element where none had applied.

The legislative history, context and purpose behind section 18-5-902 resolve this ambiguity and further demonstrate the General Assembly did not silently intend to limit identity theft to those particularly culpable offenders who knew they were exploiting the information “of another”.

B. The legislative context and drafter's statements belie Defendant's strained construction.

In addition to arguing against any consideration of the legislative context of section 18-5-902 or the consequences of his proffered construction,⁵ Defendant claims these interpretive tools support his position because they do not expressly disclaim it (*see* AB pp. 27-34).

This is incorrect. The lack of any legislative discussion, mention, or allusion to his extraordinarily narrow construction of the identity theft statute instead demonstrates the General Assembly intended that section 18-5-902 generally prohibit the exploitation of real victims' information (and thereby combat the resulting harm).

To fulfill its fundamental responsibility to determine and give effect to the General Assembly's intent, this Court considers the legislature's object in enacting legislation, the circumstances under which it was passed, and the "mischief" it was designed to address. *See Hernandez*, 250 P.3d at 572 ("this court 'strive[s] to give effect' to

⁵ *See* AB pp. 26-27 (criticizing the court of appeals for considering legislative history).

legislative intent ‘and adopt[s] the statutory construction that best effectuates the purpose[] of [the] legislative scheme’”) (quoting *Spahmer v. Gullette*, 113 P.3d 158, 162 (Colo. 2005)); *Cross*, 127 P.3d at 73 (“Often the best guide to legislative intent is the context in which the statutory provisions appear . . .”); §2-4-203, C.R.S. (2014).

Here, as discussed in the Opening Brief, the legislative context demonstrates the General Assembly intended section 18-5-902 to prohibit the exploitation of real victims’ personal information (*see* OB pp. 10-14). At the committee hearings, the discussion focused on the substantial harms to Colorado citizens who had their personal information exploited (*See, e.g.*, HB 06-1326, House Judiciary Committee (2/23/06) at 8:20-8:38, 14:10-14:36, 34:24-37:00, 32:00-33:08; Senate Judiciary Committee (4/24/06) at 3:45-4:00, 12:45-13:30). For example, one witness testified it takes victims 600 hours of effort to clear their names and a victim testified about his own experience of dealing with threats from bill collectors for debts incurred by others who had misappropriated his personal information (*see* HB 06-1326, House Judiciary Committee (2/23/06) at 35:00-37:00, 25:00-26:45; *see*

also Senate Judiciary Committee (4/24/06) at 3:45-4:00 (a witness stating it takes victims two to four years and approximately \$1,400 to address the problems caused when their identifying information is misused).

Against this background, section 18-5-902's primary author urged the legislature pass this bill with the "of another" statutory definition that focused this new offense on the real people and businesses victimized by this crime (*see* HB 06-1326, House Judiciary Committee (2/23/06) at 14:10-14:43 (highlighting this focus on real victims as the distinction between the new statute and the preexisting and inadequate criminal impersonation statute); Senate Judiciary Committee (4/24/06) at 13:45 (same)). Emphasizing this distinguishing characteristic, proponents touted the new identity theft statute as a win for consumers that provides a better tool for addressing the devastating effects to victims and the difficulties in prosecuting ID theft rings, particularly with the 21st century nature of this crime and its online components (*see, e.g.*, HB 06-1326, House Second Reading (4/11/06) at 3:09-3:42; House Judiciary Committee (2/23/06) at 10:15-12:15, 1:00-2:45, 32:00;

Senate Second Reading (5/2/06) at 1:16-1:34). *See also, e.g.,* Kristin Finklea, *Identity Theft: Trends and Issues* pp. 12-13, 20-23 (Congressional Research Service 2014) (noting that increasing globalization and the expansion of advanced technology has contributed to difficulties in prosecuting identity thieves, particularly because they often operate as parts of multi-jurisdictional criminal networks and use data breaches to compile personal identifying information) (copy attached); *IRS Says Identity Thieves Accessed Tax Transcripts for More Than 100,000 Taxpayers*, Forbes, May 26, 2015 (discussing a recent sophisticated hacking attack on the IRS that involved the use of criminal databases that contained victims' personal information).⁶

Taken together with its overwhelming support (52 co-sponsors), this legislative background indicates the General Assembly intended section 18-5-902 to broadly protect Colorado citizens from the use of their personal identifying information – without any limitation based

⁶ Available at:

<http://www.forbes.com/sites/kellyphillipserb/2015/05/26/irs-says-identity-thieves-accessed-tax-transcripts-for-more-than-100000-taxpayers/print/>

on whether identity theft rings or other perpetrators knew whose information they exploited. This construction is also consistent with the venerable “mischief rule”, which considers:

1st. What was the common law before the making of the Act. 2nd. What was the mischief and defect for which the common law did not provide. 3rd. What remedy the Parliament that resolved and appointed to cure the disease of the commonwealth. And, 4th. The true reason of the remedy; and then the office of all the Judges is always to make such construction as shall suppress the mischief, and advance the remedy, and to suppress subtle inventions and evasions for continuance of the mischief.

Heydon’s Case, 76 Eng. Rep. at 638. Applied to section 18-5-902: (1) before 2006, Colorado was one of the few states that had no identity theft statute and only addressed the use of “false or fictitious” identities through criminal impersonation; (2) criminal impersonation provided an inadequate remedy and did not address the substantial harm to real victims; (3) the General Assembly responded by passing 18-5-902, which more harshly penalizes the use “of another” natural person’s identifying information; and (4) the law enforcement and consumer rights supporters of section 18-5-902 pushed for the identity theft statute to

protect the public against those who would use another person's information for their own gain.

Given these factors, this Court should construe section 18-5-902 to prohibit the conduct at issue (the knowing use of personal identifying information) and avoid "subtle inventions and evasions" like Defendant's proffered construction. The most obvious consequence of Defendant's construction is that ensures section 18-5-902 is ineffective in protecting victims while creating special protections and defenses for offenders who can claim ignorance about the origin of the information they exploit.⁷ Thus, Defendant's construction is contrary to our system's first principles of statutory construction.

Finally, just as important as the content of the legislative history is what is missing – any suggestion that the General Assembly intended to limit identity theft to those cases where the offender specifically knew he was victimizing a real person. Under the "dog didn't bark"

⁷ Such ignorance is easy to claim and difficult to disprove, particularly given the online criminal databases and secondary markets for personal identifying information. Defendant's construction directly encourages such identity theft markets.

cannon, courts attribute significance where the legislative history contains no discussion, mention or allusion to the critical change or limitation of a law embodied by a party's proposed interpretation. *See* Jacob Scott, *Codified Cannons and the Common Law of Interpretation*, 98 Geo. L.J. 341, 379 n. 208 (Jan. 2010). Here, despite hours of hearings and opportunities to make such a record, no one suggested that section 18-5-902 would apply to only the most culpable offenders or that criminal impersonation should be applied to the misappropriation "of another[s]" identifying information in all other instances.

Thus, for these reasons, the Court should reject Defendant's hypertechnical efforts to thwart the legislature's intent and hold section 18-5-902 prohibits the knowing use of personal identifying information whenever it actually belonged to (and therefore harmed) a real victim.

II. There was a logical connection between the Defendant's repeated use of the victim's Social Security number and the jury's conclusion that he knew it belonged to a real person.

Jury verdicts are entitled to deference and can only be vacated for insufficient evidence where there is no logical connection between the evidence and the jury's conclusion. *See Clark v. People*, 232 P.3d 1287, 1291, 1288-89 (Colo. 2010); *People v. Bennett*, 183 Colo. 125, 515 P.2d 466, 469 (1973).

Here, the jury concluded Defendant knew the Social Security number he had consistently used to obtain wages belonged to a real person where: he used a Colorado woman's Social Security number to work at nearby restaurants; he used a counterfeit Social Security card with his name and her number; a manager testified that her restaurant's payroll system rejected inaccurate or incomplete personal identifying information; he used the victim's Social Security number on tax forms and had his wages deducted accordingly; and Defendant successfully used the same victim's Social Security number to obtain

wages from at least four different employers over a five-year period (*see* PR. Vol. 4 pp. 200-01; OB pp. 20-25).

Defendant maintains no rational juror could reach this conclusion because it does not disprove his unsuccessful trial theory that he believed S.G.'s Social Security number was a random series of nine numbers (*see* AB pp. 37-48). But like the court of appeals opinion, Defendant's arguments ask this Court to reweigh the evidence in isolation instead of "view[ing it] as a whole and in the light most favorable to the prosecution." *See Clark*, 232 P.3d at 1288.

First, Defendant asserts that his use of a Broomfield woman's Social Security number to work in north metro Denver is a mere coincidence and that nothing suggests Defendant "or anyone else" would know "that the number here was associated with or connected to Colorado" (*see* AB pp. 38-39). To the contrary, the close proximity between the victim and Defendant is circumstantial evidence against his "random series of nine numbers" theory because there are 1,000,000,000 possible combinations of an SSN and the chances that a random combination would correspond to real person who lives down

the road are infinitesimal. Far more likely is that Defendant selected this number based on its geographical association. After all, the number's "523" prefix is based on the Colorado zip code S.G. had when she applied for her card (*see* Exhibits 4 (Defendant's I-9 Employment Eligibility Verification), 5 (copy of Defendant's fraudulent Social Security Card taken in conjunction with form I-9)). *See also* SSA, Social Security Number Allocations, available at <http://www.ssa.gov/employer/stateweb.htm>.⁸

Second, Defendant claims no evidence implied payroll systems would reject inaccurate Social Security numbers and other individuals successfully worked for years using numbers that were not assigned to anyone (*see* AB pp. 39-40, 43 (citing a 2005 news article regarding the Social Security Administration's "earning suspense file" containing tax withholdings submitted under fictitious SSNs)). But these challenges to the weight of the evidence and inferences to be drawn from it cannot

⁸ To combat identity theft, in 2011 the Social Security Administration discontinued this practice and eliminated the geographical significance of the first three digits of the SSN. *See* SSA, Social Security Number Randomization, available at <http://www.ssa.gov/employer/randomization.html>

justify vacating the jury's verdict where: (1) a restaurant manager testified that the payroll system would not pay wages if employees provided incorrect or incomplete information, including Social Security numbers (*see* PR. Vol. 4 p. 19; Exhibit 3 (Defendant's W-4 tax withholding form));⁹ and (2) the Social Security Administration itself audits withholdings associated with fictitious SSNs (the "earning suspense file") and contacts employers with "No Match" letters to address W-2 submissions that could not be matched to a real individual's earnings report. *See* SSA, Social Security Testimony Before Congress (Feb 16, 2006);¹⁰ *see also* Finklea, *supra* at pp. 15, 20 (discussing the SSA's role in stopping identity theft and the problems caused by employment identity fraud). While the SSA's recent efforts to address the earnings suspense file will now flag contributions made under counterfeit Social Security numbers, this program will not identify those (like Defendant) who misappropriate real Social Security

⁹ Though unclear from the record, this may have included the rejection of presumptively invalid SSNs like those starting "000". *See supra* Social Security Number Allocations.

¹⁰ Available at http://www.ssa.gov/legislation/testimony_021606.html

numbers.¹¹ Put simply, those who work under a real person's information are less likely to be caught by the Social Security Administration – making valid Social Security numbers more valuable to unauthorized workers and justifying the effort to create counterfeit Social Security cards using this information.

Third, Defendant maintains the jury could not infer that he knew valid Social Security numbers were required for employment or that his bi-weekly tax deductions would be attributed to the Social Security number he used on employment forms (*see* AB pp. 41-44). There are three problems with this argument: (1) it incorrectly suggests the prosecution was required to present evidence about federal employment and tax withholdings law and then prove Defendant's awareness of these laws (*see* OB pp. 22-24); (2) it relies on an incorrect and outdated belief that there is no government monitoring of the wage withholdings on counterfeit Social Security numbers – instead, these are more likely to be questioned by the SSA than wages from misappropriated SSNs;

¹¹ Such misappropriations can be caught by employers who use the voluntary E-Verify system that checks SSNs against names and other characteristics.

and (3) it overrules the jury's judgment in selecting one inference (Defendant, like every other worker, knew the deductions from his paychecks were being attributed to the Social Security number he was using) over its less likely counterpoint (Defendant had no idea he had to provide a valid SSN or that the deductions from every paycheck were attributed to its owner) (*see* OB pp. 23-24; *see also* PR. Vol. 4 pp. 93-94 (trial court relying on the reasonable inferences from the wage deductions evidence when denying Defendant's motion for acquittal)).

Fourth, Defendant contends the jury could not infer he knew he was using a valid Social Security number based on his success in obtaining wages because he did not test it against different types of systems (*e.g.*, by applying for a passport, driver's license or other government document) (*see* AB pp. 44-47). But this (again) goes to the strength of available inferences regarding Defendant's knowledge rather than the legal insufficiency of the evidence. The People agree the inference that Defendant knew he was exploiting a real person's identifying information would be stronger if he had used it to successfully obtain multiple types of benefits. Nevertheless, the same

(albeit weaker) inference arises from Defendant's conduct here because he repeatedly and successfully used S.G.'s Social Security number to obtain wages from four different employers over a five-year period; and did so without triggering a "No Match" letter from the Social Security Administration as he could with a fictitious Social Security number.

Thus, while there was not overwhelming the evidence that Defendant knew he was exploiting a real person's Social Security number, there was sufficient circumstantial evidence for a rational juror to reach this conclusion. The jury is uniquely suited to make this determination and its verdict should not be overridden on a cold record based on Defendant's disputes as to the weight of a piece of evidence or the strongest inferences he believes should be drawn from it.

CONCLUSION

For these reasons, this Court should reverse and hold: (1) section 18-5-902 prohibits the knowing use of personal identifying information whenever it actually belonged to a real victim; and (2) there was sufficient evidence to sustain the jury's verdict.

CYNTHIA H. COFFMAN
Attorney General

/s/ Kevin E. McReynolds

KEVIN E. MCREYNOLDS, 40978*
Assistant Attorney General
Criminal Appeals Section
Attorneys for the People of the State of
Colorado
*Counsel of Record

CERTIFICATE OF SERVICE

This is to certify that I have duly served the within **PEOPLE'S
REPLY BRIEF** and attachment upon **ANDREW C. HEHER**, Deputy
State Public Defender, and all parties herein via Integrated Colorado
Courts E-filing System (ICCES) on June 4, 2015.

/s/ Tiffiny Kallina



**Congressional
Research Service**

Informing the legislative debate since 1914

Identity Theft: Trends and Issues

Kristin Finklea

Specialist in Domestic Security

January 16, 2014

Congressional Research Service

7-5700

www.crs.gov

R40599

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

Introduction.....	1
Definitions of Identity Theft	2
Theft vs. Fraud.....	3
Knowledge Element	3
Legislative History.....	4
Identity Theft Assumption Deterrence Act	4
Identity Theft Penalty Enhancement Act.....	4
Identity Theft Enforcement and Restitution Act of 2008	5
Identity Theft Task Force.....	5
Recommendations	5
Legislative Recommendations.....	6
Red Flags Rule.....	7
Trends in Identity Theft	9
Perpetrators.....	12
Investigations and Prosecutions.....	13
Federal Bureau of Investigation (FBI)	14
United States Secret Service.....	14
United States Postal Inspection Service	14
Social Security Administration Office of the Inspector General (SSA OIG)	15
Immigration and Customs Enforcement.....	15
Department of Justice.....	15
Domestic Impact.....	17
Credit Card Fraud.....	19
Document Fraud.....	19
Employment Fraud.....	20
Data Breaches and Identity Theft	20
Potential Issues for Congress.....	23
Identity Theft Prevention.....	24
Securing Social Security Numbers.....	24
Effects of Data Breaches	25
Deterrence and Punishment.....	26

Figures

Figure 1. FTC Consumer Complaint Data.....	11
Figure 2. FTC Identity Theft Complaint Data	12
Figure 3. Federal Identity Theft and Aggravated Identity Theft Cases.....	16
Figure 4. FTC Identity Theft Complaints, 2012	18
Figure 5. Total Number of Reported Data Breaches and Records Affected	21

Contacts

Author Contact Information..... 27

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., 2nd 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.

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.

Theft vs. Fraud

Identity theft and identity fraud are terms that are often used interchangeably. Identity fraud¹² is the umbrella term that refers to a number of crimes involving the use of false identification—though not *necessarily* a means of identification belonging to another person. Identity theft is the specific form of identity fraud that involves using the personally identifiable information of someone else. Both identity fraud and identity theft are crimes often committed in connection with other violations, as mentioned above. Identity theft, however, may involve an added element of victimization, as this form of fraud may directly affect the life of the victim whose identity was stolen in addition to defrauding third parties (such as the government, employers, consumers, financial institutions, and health care and insurance providers, just to name a few). This report, however, maintains a focus on identity theft rather than the broader term of identity fraud.

Knowledge Element

Another definitional issue is one that 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

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.

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.

Legislative History¹⁵

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 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.

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.

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.

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 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.

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

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.

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 statutes to more effectively prosecute and punish identity theft-related offenses by

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

²⁴ Ibid.

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 Rule²⁵

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 creditors²⁷ and financial institutions²⁸ 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

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.

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 (continued...)”

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 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.

(...continued)

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>.

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>.

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 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

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.

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.

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 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

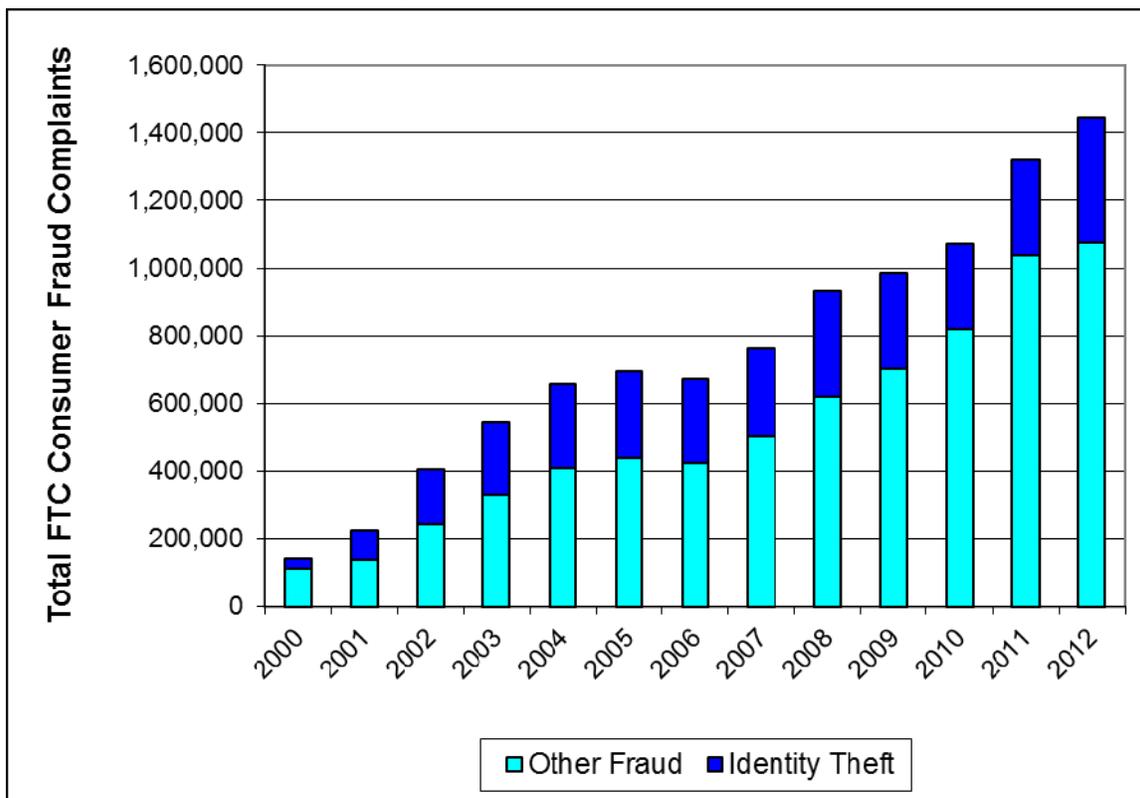
⁴² Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013.

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>.

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 1. FTC Consumer Complaint Data

Identity Theft and Other Fraud for 2000-2012



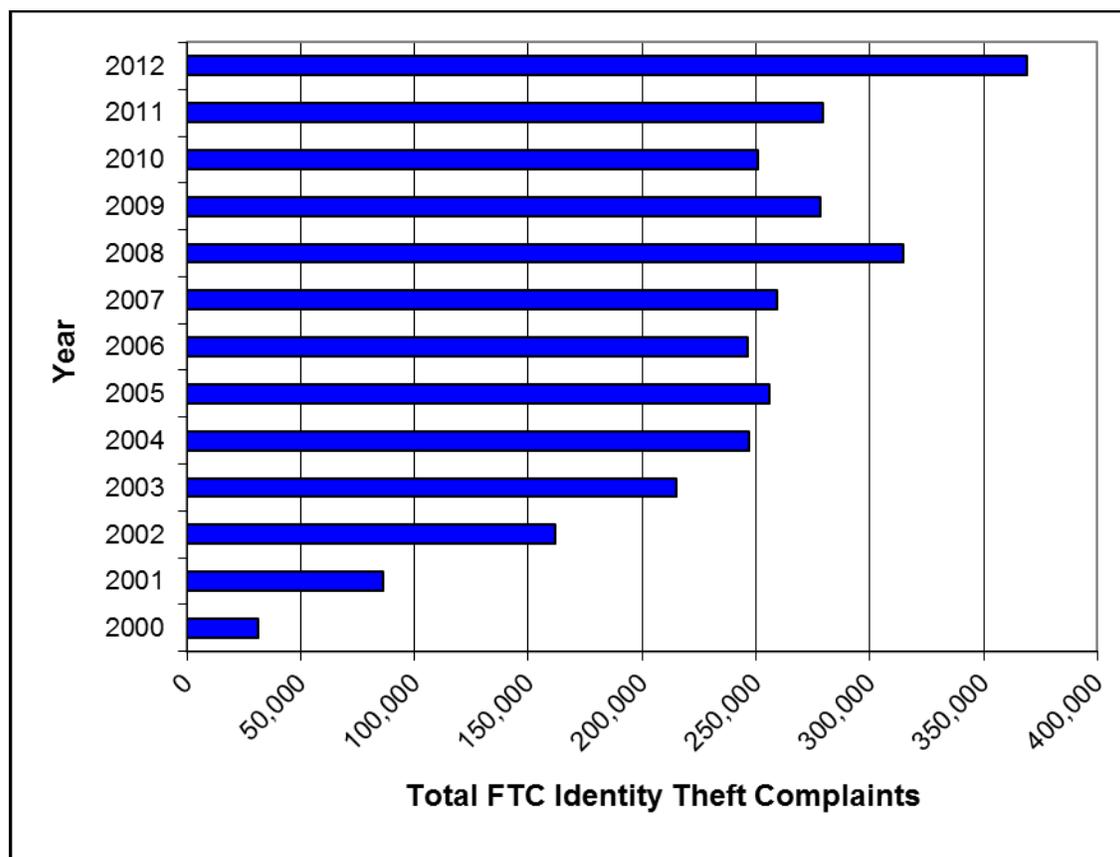
Source: CRS presentation of FTC Identity Theft Clearinghouse data. Annual reports for each calendar year are available at <http://www.ftc.gov/enforcement/consumer-sentinel-network/reports>.

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.

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

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>.

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 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

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>.

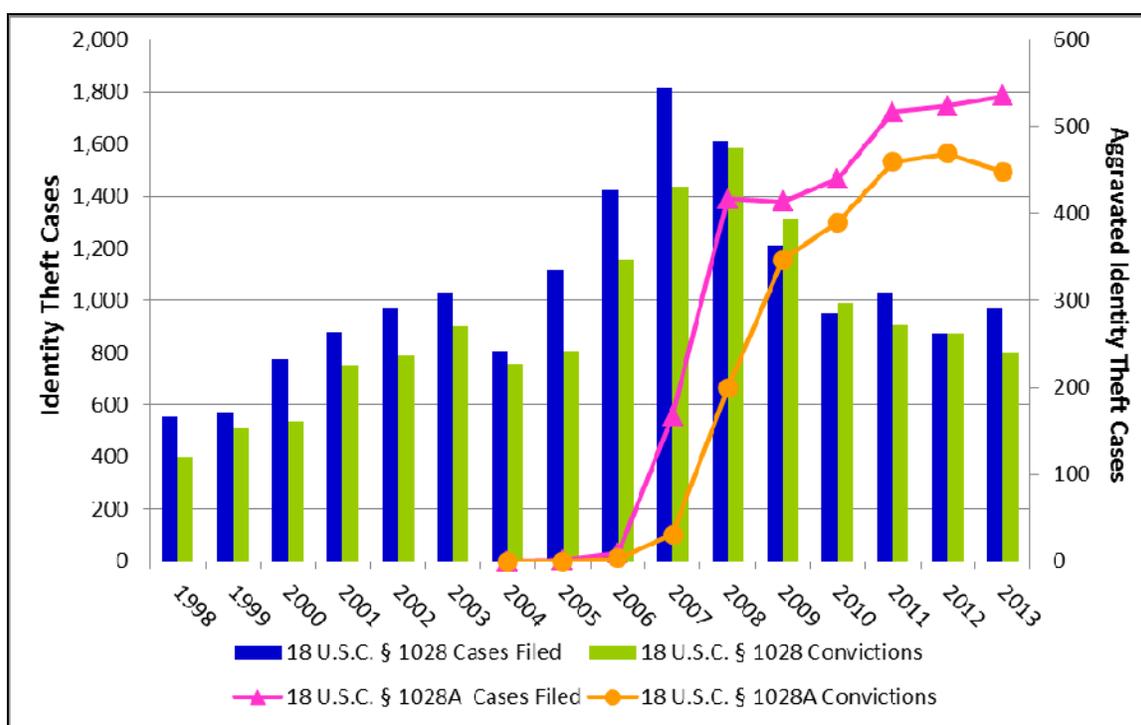
⁶⁰ Information provided to CRS by the Social Security Administration, Office of the Inspector General, Office of Congressional Affairs.

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

according to the charging statutes. Identity theft cases fall under several programmatic categories—including white collar crime and immigration—which also contain several other crimes. Thus, trends in federal identity theft and aggravated identity theft cases may be better tracked by the number of total cases referred to and prosecuted by the USAOs, irrespective of the referring agency.

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 filed⁶² 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

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.

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 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.

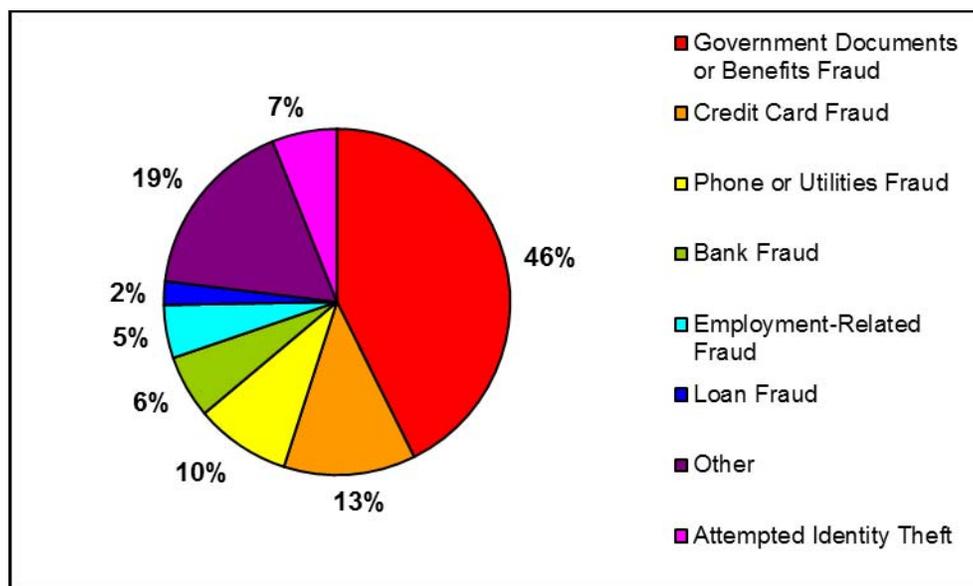
⁶³ Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, February 2013; Erica Karrell and Lynn Langton, *Victims of Identity Theft, 2012*, U.S. Department of Justice, Bureau of Justice Statistics, NCJ 243779, December 2013.

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 Fraud⁶⁹

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 Fraud⁷³

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 immigrants⁷⁴ 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,

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/2002/050202agidthetranscript.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>.

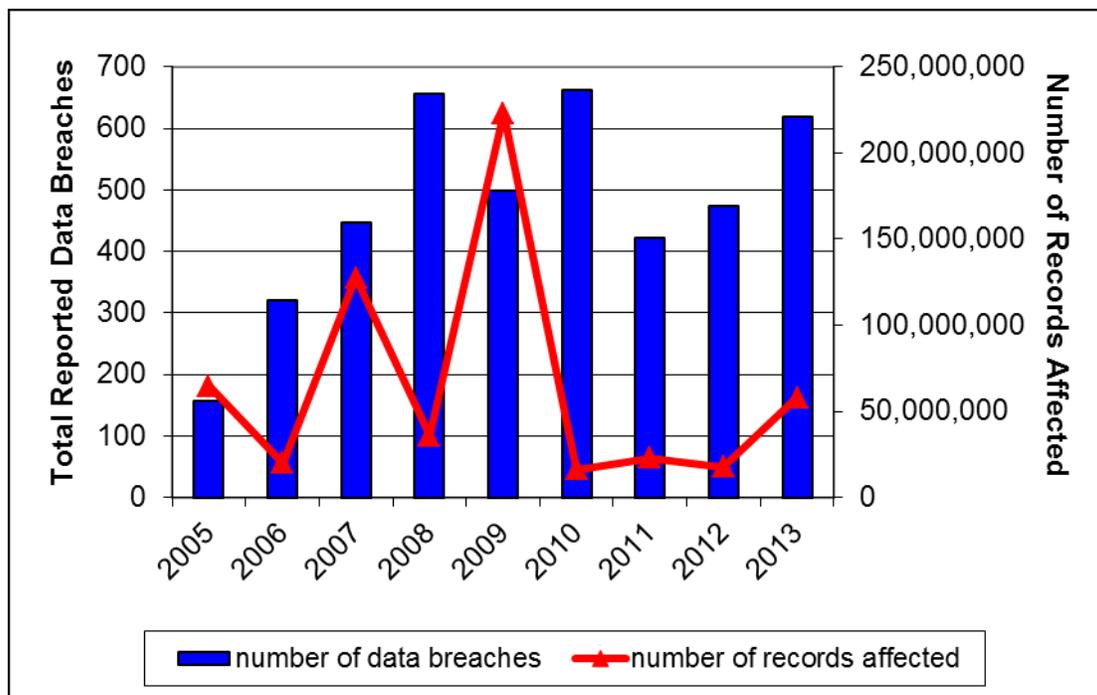
⁷⁶ Federal Bureau of Investigation, *Three Accused of Operating Fake ID Ring Plead Guilty*, September 4, 2013, <http://www.fbi.gov/richmond/press-releases/2013/three-accused-of-operating-fake-id-ring-plead-guilty>.

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>.

there were 619 reported breaches).⁷⁸ **Figure 5** illustrates this trend. Breaches are recorded across 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

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 ITRC indicates that the criteria for qualifying as a data breach is “[a]ny name or number that may be used, alone or in conjunction with other information, to identify a specific individual, including: name, Social Security number, date of birth. Banking or financial account number, credit card or debit card number with or without a PIN, official state or government issued driver’s license or identification number, 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.

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 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

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>.

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/IIRC-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.

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 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.

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

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.

Identity Theft Prevention

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

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

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.

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 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

⁹⁵ 42 U.S.C. §13925.

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.

breaches. However, this proportion is truly unknown because most victims of identity theft do not know precisely how their personally identifiable information was acquired. In order to prevent any proportion of identity theft that may result from data breaches, or to mitigate the extent of the damage resulting from breach-related identity theft, Congress may wish to consider whether to strengthen data breach notification requirements. Such requirements could affect both the notification of the relevant law enforcement authorities as well as the notification of the individual whose personally identifiable information may be at risk from the breach.

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

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 (continued...)

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 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 Contact Information

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

(...continued)

<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.

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