What's the Use?: Interpreting the Term "Uses" in the Aggravated Identity Theft Provision

Shang-Chi Andrew Liu†

The Identity Theft Penalty Enhancement Act (ITPEA) increases penalties for crimes that involve the unlawful use of another person's identifying information. A subsection of the ITPEA—the aggravated identity theft provision—imposes a mandatory two-year sentencing enhancement on a defendant who "uses" a means of identification of another person during and in relation to a predicate felony. Currently, federal circuit courts disagree about whether the term "uses" in the statute is ambiguous and whether the rule of lenity should consequently apply to narrow its reach. On the one hand, courts that have held the statute to be ambiguous apply the rule of lenity to hold that a defendant qualifies for the enhancement only if the defendant has directly impersonated another person. On the other hand, courts that have held the statute to be unambiguous reason that the plain text of the statute demands that the defendant need only generally misuse another's information in the facilitation of fraud.

This Comment argues that the rule of lenity is improper in the context of the aggravated identity theft provision because a variety of interpretive tools are available and operative. For that reason, courts should apply the statute in accordance with its broad plain meaning by construing "uses" as requiring only general misuse of another person's identifying information. This reading draws support from an analogous case in a comparable criminal context, interactions between interpretive canons, and legislative history found in the amendment notes to the ITPEA. This reading also provides practical benefits for courts assessing these issues in a contemporary technological landscape rife with digital political dissent and vigilante hacktivism.

† B.A. 2020, University of California, Los Angeles; J.D. Candidate, The University of Chicago Law School. Many thanks to the editors and staff of the *University of Chicago Law Review* for their helpful advice and insight.

INTRODUCTION

In the cold open of an episode of *The Office*, Jim Halpert impersonates coworker Dwight Schrute by donning a cream-colored shirt, wire-frame glasses, and middle-parted hair.[1] Though he meets the display with initial displeasure, Dwight eventually retorts that "imitation is the most sincere form of flattery."[2] Jim's antics ultimately prove overbearing, however, as Dwight goes on to famously exclaim, "Identity theft is not a joke, Jim! Millions of families suffer every year!"[3]

There is truth to Dwight's words. According to a Federal Trade Commission (FTC) report, identity crimes resulted in a loss of $3.3 billion for U.S. consumers in 2020.[4] The COVID-19 pandemic has exacerbated this problem by indirectly giving rise to novel opportunities for identity-related scams,[5] including stealing federal stimulus payments, impersonating the Centers for Disease Control and Prevention, and peddling sham vaccinations. As

---

1 *The Office: Product Recall* (NBC Apr. 26, 2007).

2 *Id.*

3 *Id.*

4 FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 5 (2020).

5 *See Fraud Alert: COVID-19 Scams*, U.S. DEP'T OF HEALTH AND HUM. SERVS. OFF. OF INSPECTOR GEN. (Feb. 2, 2022), https://perma.cc/57Z5-CK6G; Safia Samee Ali, *Pop-Up Covid Testing Sites May Be Rife for Identity Theft, Experts Say*, NBC NEWS (Jan. 8, 2022), https://perma.cc/V9QC-EFKH; *cf.*, Press Release, Dep't of Just., *Licensed Pharmacist Charged with Hoarding and Price Gouging of N95 Masks in Violation of Defense Production Act* (May 26, 2020), https://perma.cc/E3PE-TGP6.

a result, the FTC received almost 1.4 million identity theft complaints in 2020, a 113% increase from the previous year.[6]

The United States had addressed the threat of identity crimes for decades well before these contemporary developments. During the technology boom of the late nineties, Congress enacted the Identity Theft and Assumption Deterrence Act of 1998[7] (ITADA), which made identity theft a federal crime. Six years later, Congress enacted the Identity Theft Penalty Enhancement Act of 2004[8] (ITPEA). A subsection of the ITPEA targets aggravated identity theft: the knowing transfer, possession, or *use*, without lawful authority, of a means of identification of another person during and in relation to a predicate felony.[9] This aggravated identity theft provision imposes a mandatory two-year term of imprisonment in addition to the punishment for the underlying predicate felony.[10]

The aggravated identity theft provision is easy to apply in simple cases but poses challenges in more complex scenarios. For a simple example, consider a defendant—an IT employee of a graduate program—who obtains the Social Security number of an applicant through the program's admissions portal. Without the applicant's consent, the defendant uses the Social Security number to impersonate the victim and obtain loans and lines of credit in the victim's name. In this case, the predicate felony of a false statement under the Social Security Act[11] is specifically enumerated under 18 U.S.C. § 1028A(c), thereby mandating the two-year sentencing enhancement for identity crimes that occur during the underlying offense.[12] The means of identification at issue is the Social Security number itself. Put another way, the IT employee uses the applicant's identification without lawful authority in relation to Social Security fraud, the associated predicate felony. This situation embodies the traditional idea of identity theft—impersonation—and clearly qualifies as a "use" of a means of identification for purposes of the aggravated identity theft provision.

For a more complex example, consider a health-care fraud scheme. An owner of a massage clinic makes an arrangement

---

6 *Compare* FED. TRADE COMM'N, *supra* note 4, at 7, *with* FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 7 (2019).

7 Pub. L. No. 105-318, 112 Stat. 3007.

8 Pub. L. No. 108-275, 118 Stat. 831 (codified at 18 U.S.C. § 1028A).

9 18 U.S.C. § 1028A(a)(1).

10 18 U.S.C. § 1028A(a)(1).

11 Pub. L. No. 74-271, 49 Stat. 620 (codified in scattered sections of 42 U.S.C.).

12 *See* 18 U.S.C. § 1028A(c)(11).

with a physical-therapy company. Under the arrangement, the owner amasses a set of customers and—with the customers' consent—shares their Medicare information with the company. For context, Medicare pays for physical therapy but does not pay for massages. The company has a Medicare provider number that allows it to submit claims for payments. The parties agree that the owner will supply the infrastructure of a clinic while the company will bill Medicare for physical-therapy services that, in reality, are luxurious massage sessions. In this case, the specific predicate felony is health-care fraud under 18 U.S.C. § 1028A(c)(4). The means of identification at issue is the Medicare information. As a result of this practice, Medicare pays over $2.9 million to the company, and the owner receives over $1.6 million.[13]

Several questions emerge in the second situation that did not arise in the first. The owner did not impersonate the customers, and his actions do not fall into the traditional understanding of identity theft. But does the owner's collection and sharing of customers' Medicare information constitute "use" of a "means of identification of another person," given the information's general role in facilitating the health-care fraud scheme? Or do the owner's actions fall outside the scope of the provision because the owner did not attempt to directly pass himself off as the customers? In addition, does the fact that the customers initially consented to the sharing of their Medicare information have any bearing on the outcome?

These questions have led to divergent approaches in the application of the aggravated identity theft provision in circuit courts. Principally, the circuits disagree about whether the term "uses" in the aggravated identity theft provision is ambiguous and whether the rule of lenity should consequently apply to narrow the statute's reach. Under the minority interpretation followed by the First, Sixth, and Ninth Circuits, the term is indeed ambiguous and so the rule of lenity applies. Therefore, for a defendant to use a means of identification of another person, the defendant must directly impersonate another person. Under the majority interpretation followed by the Fourth, Fifth, Eighth, Eleventh, and D.C. Circuits, however, the term is not ambiguous and so the rule

---

[13] For a case that reflects this set of facts, see *United States v. Hong*, 938 F.3d 1040, 1043–45 (9th Cir. 2019). For additional discussion of the case, see Part II.A.1.

of lenity does not apply. Accordingly, in order to violate the aggravated identity theft provision, the defendant need only generally misuse another's information in the facilitation of fraud.

Some circuits also disagree about how to interpret the phrase "another person," though this issue arises in fewer cases and the courts give this topic less attention. Under the minority interpretation followed by the Seventh Circuit, for a defendant to use a means of identification of "another person," the defendant must steal the information from the victim. Under the majority interpretation followed by the Fourth, Eighth, and Ninth Circuits, however, the term "another person" can include those who consented to the defendant using their identifying information.

This Comment uses interpretive tools to determine how to apply the aggravated identity theft provision, shedding new light on these divergent approaches. First, I employ textual analysis and examine *Smith v. United States*,[14] an analogous case that has wrangled with similar statutory language. I observe that, according to the surplusage canon, "uses" should have a meaning so as not to duplicate the meanings of the other two verbs in the provision. Second, I draw upon the House Report and amendment notes to the ITPEA, which support a broader interpretation of the statute. Furthermore, as a matter of policy, the fact that the aggravated identity theft provision enumerates specific and limited categories of predicate felonies quells the concerns that a broader reading of the statute would result in its application to situations beyond those that Congress had considered while drafting the ITADA and the ITPEA.

This Comment proceeds in four parts. Part I provides an overview of the ITADA and its shortcomings, describing how Congress attempted to bolster identity-crime laws through the ITPEA. Part II outlines the divergent approaches at the circuit level regarding both the ambiguity of the aggravated identity theft provision's language and the significance of the owner's consent. Part III employs interpretive tools to determine how to apply the aggravated identity theft provision, arguing that applying the rule of lenity is improper in this particular context. Part IV examines the practical benefits of relying on the unambiguous, though broad, meaning of the aggravated identity theft provision as it applies to digital political dissent and vigilante hacktivism in online ecosystems. Using the majority interpretation, courts

---

[14] 508 U.S. 223 (1993).

are better equipped to employ the statute in a contemporary technological landscape.

I. BACKGROUND AND RELEVANT LAW

As noted above, identity crimes have long been threats to society. Part I.A provides the historical backdrop against which Congress enacted the ITADA. Taken as a whole, this enactment reflected Congress's intent to develop and expand its legislation regarding identity theft to adapt to a changing social and technological environment during the technology boom of the late nineties. Part I.B notes the shortcomings of the ITADA and how Congress attempted to bolster identity theft laws through the ITPEA. As a general matter, the ITPEA reflected Congress's wariness of costly recidivism. The historical development of the ITADA and ITPEA ultimately established the statutory and policy framework in which the aggravated identity theft provision operates and continues to influence the way it should operate.

A. The Identity Theft and Assumption Deterrence Act

Prior to Congress's enactment of the ITADA in 1998, which made identity theft a federal crime, prosecutors generally charged identity-theft crimes under state law through false-personation statutes.[15] These state statutes made it illegal to falsely assume the identity of another to gain a benefit or avoid an expense.[16] Oftentimes, they were outdated and ill-equipped to deal with technological advances—namely, new online financial crimes, such as credit-card fraud, that the development of the internet enabled. Given that these online crimes often occurred across state lines, the lack of a functioning and effective federal

---

[15] *See, e.g.*, *Identity Theft and Financial Fraud*, OFF. FOR VICTIMS OF CRIMES (Oct. 2010), https://perma.cc/6X8A-PMVZ.

[16] *See, e.g.*, 720 Ill. Comp. Stat. § 5/17-2(a)(2.5) (2017) ("A person commits a false personation when he or she knowingly and falsely represents himself or herself to be: [ ]another actual person and does an act in such assumed character with intent to intimidate, threaten, injure, defraud, or to obtain a benefit from another."); Fla. Stat. § 817.02(1) (2021) ("Whoever falsely personates or represents another person, and in such assumed character: [ ] [r]eceives any property intended to be delivered to that person, with intent to convert the same to his or her own use . . . shall be punished as if he or she had been convicted of larceny."); N.Y. Penal Law § 190.23 (2014) ("A person is guilty of false personation when . . . he or she knowingly misrepresents his or her actual name, date of birth or address to a police officer or peace officer with intent to prevent such police officer or peace officer from ascertaining such information.").

law that addressed these crimes made it difficult to deter their rapid proliferation.

In response, Congress passed the ITADA, which amended 18 U.S.C. § 1028 (the identity fraud provision) to bolster the laws governing identity-related crime. Specifically, it authorized punishment for whoever "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit . . . any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[17] In this context, the term "means of identification" refers to any document, name, or number that may be used to identify a specific individual, including any government issued identification, biometric data, or electronic identification number.[18] This offense can carry a maximum term of fifteen years of imprisonment, a fine, and criminal forfeiture of any personal property used to commit the offense.[19]

From a legislative perspective, the ITADA sought to address growing concerns associated with the rise of new technologies.[20] According to the relevant Senate Report, the ITADA serves two primary purposes: (1) "to extend [the identity fraud provision], which criminalizes fraud in connection with identification *documents*, to cover the unlawful transfer and use of identity *information*" and (2) "to recognize the individual victims of identity theft crimes, and establish their right to restitution to include all costs related to regaining good credit or reputation."[21] The report also noted that "criminals do not necessarily need a document to assume an identity; often they just need the information itself to facilitate these types of crimes."[22] Thus, by amending the identity fraud provision, the drafters hoped that "this statute [would] keep pace with criminals' technological advances."[23]

---

17 18 U.S.C. § 1028(a)(7).

18 18 U.S.C. § 1028(d)(7).

19 18 U.S.C. § 1028(b).

20 *See* President William J. Clinton, Statement on Signing the Identity Theft and Assumption Deterrence Act of 1998, 5 U.S.C.C.A.N. 703 (Oct. 30, 1998) ("This legislation will enable the United States Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this type of crime, which can financially devastate its victims. . . . As we enter the Information Age, it is critical that our newest technologies support our oldest values.").

21 S. REP. NO. 105-274, at 4 (1998) (emphasis in original).

22 *Id.* at 5.

23 *Id.*

Of particular note, the ITADA established identity theft as an independent crime, a measure originally meant to combat individuals who stole others' means of identification to extend their own credit lines.[24] While the law previously focused on credit grantors that suffered monetary losses as the primary victims of credit card fraud, the ITADA recognized individuals whose identities were stolen as victims who could now seek direct restitution upon conviction of the perpetrator. In this way, the amended language of the identity fraud provision broadened the law's scope to encompass the losses of individuals in addition to those sustained by banks and other financial institutions.

Consider a situation in which an actor uses the personal identifying information of a set of victims to obtain a sizable loan. Before the ITADA, the perpetrator would be charged under false-personation statutes, among other violations, and any restitution would only be available to the banks involved. The individual victims would have to spend considerable time restoring their credit ratings and clearing their names but would not have any legal recourse against the perpetrator.[25] The ITADA, however, created new mechanisms that provided for restitution for the individual victims to compensate them for harms to reputation, inconvenience, and other consequences.[26] To further help victims recover, the ITADA also created the Identity Theft Data Clearinghouse, an online fraud complaint database operated by the FTC.[27]

B. The Identity Theft Penalty Enhancement Act

In 2004, Congress enacted the ITPEA to "address[ ] the growing problem of identity theft."[28] Although the ITADA recognized identity theft as a federal crime and provided specific remedies, it struggled to keep pace with the rapidly increasing use of the internet and electronic devices as the United States entered the

---

[24] *See generally* 18 U.S.C. § 1028.

[25] For example, during a legislative hearing, factory worker Bob Hartle testified that the felon who stole his identity taunted him over the phone by saying that "he would continue to pose as Hartle for as long as he wanted since using his identity was not a crime." S. REP. NO. 105-274, at 6 (1998). The felon "caused Hartle to suffer over $100,000 of credit card debt, and bought homes and motorcycles in Hartle's name before filing for bankruptcy, also in Hartle's name." *Id.*

[26] *See id.* at 11 ("Restitution.—This provision legally acknowledges victims of identity theft by adding to section 1028 a requirement that victims who have suffered a pecuniary loss are entitled to mandatory restitution under 18 U.S.C. 3663A.").

[27] *See generally* FED. TRADE COMM'N, REPORT: FEDERAL TRADE COMMISSION OVERVIEW OF THE IDENTITY THEFT PROGRAM OCTOBER 1998–SEPTEMBER 2003 (2003).

[28] H.R. REP. NO. 108-528, at 3 (2004), *as reprinted in* 2004 U.S.C.C.A.N. 779, 779.

Information Age.[29] Following the September 11 attacks, there was increased attention to identity theft because of potential security threats. In 2003, a random sample conducted by the FTC suggested that ten million U.S. consumers were victims of identity crimes that year.[30] The FTC estimated that the loss to banks and financial institutions was approximately $47.6 billion and the costs to individual consumers was $5.0 billion.[31]

Observing these trends, Congress was concerned that the existing laws did not sufficiently deter repeat offenders, many of whom used new technology that made it easier to collect other people's information.[32] In response to these issues, Congress passed the ITPEA to penalize aggravated identity theft, defined as the use of the identity of another person in relation to the specific felony violations enumerated within the statute.[33] These limited enumerated felony violations include, for example, theft of public money, false personation of citizenship, and the misappropriation of other people's Social Security benefits.[34]

The subsection of the ITPEA that sets this into motion is 18 U.S.C. § 1028A, which created the crime of aggravated identity theft. Specifically, the aggravated identity theft provision establishes that "[w]hoever, during and in relation to [the predicate felony], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced

---

29 *See* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 674–75 (1999) (noting that the ITADA "specifically recognizes identity theft as a distinct crime of its own").

30 H.R. REP. NO. 108-528, at 4 (2004), *as reprinted in* 2004 U.S.C.C.A.N. 779, 780.

31 *Id.*

32 *See id.* at 3–4, *as reprinted in* 2004 U.S.C.C.A.N. 779, 779–80.

33 18 U.S.C. § 1028A.

34 *See* 18 U.S.C. § 1028A(c). The full set of enumerated felonies is as follows: theft of public money, property, or rewards under 18 U.S.C. § 641; theft, embezzlement, or misapplication by a bank officer or employee under 18 U.S.C. § 656; theft from employee benefit plans under 18 U.S.C. § 664; false personation of citizenship under 18 U.S.C. § 911; false statements in connection with the acquisition of a firearm under 18 U.S.C. § 922(a)(6); crimes relating to fraud or false statements under any provision other than 18 U.S.C. § 1028A or 18 U.S.C. § 1028(a)(7); mail, bank, and wire fraud under Chapter 63; nationality and citizenship fraud under Chapter 69; passport and visa fraud under Chapter 75; obtaining customer information by false pretenses under § 523 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6823; willful failure to leave the United States after deportation and creation of counterfeit alien registration cards under § 243 or § 266 of the Immigration and Nationality Act, 8 U.S.C. § 1321; immigration offenses contained in Chapter 8 of Title II of the Immigration and Nationality Act, 8 U.S.C. § 1321; and false statements relating to Social Security.

to a term of imprisonment of 2 years."[35] Put another way, engaging in an identity crime while also engaging in an enumerated predicate felony triggers the enhancement. The statute tacks on this two-year sentencing enhancement without adjusting or accounting for underlying terms of imprisonment or other enhancements.[36]

The enactment of the ITPEA was part of a broader trend of federal actions meant to protect victims' livelihoods and their financial reputations.[37] During this time, federal agencies worked with state officials to crack down on criminal networks responsible for much of the identity theft within the nation, and the Identity Theft Data Clearinghouse remained in full operation. Around the same period, Congress enacted the Fair and Accurate Credit Transactions Act of 2003[38] (FACTA), which gave consumers the right to one free credit report a year from each of the major credit reporting agencies.[39] FACTA also allowed consumers to implement fraud alerts in their credit files to stop identity-related crimes at their inception and protect their credit ratings.[40] Moreover, the aggravated identity theft provision included a specific enumerated predicate felony that criminalized the misdeeds of commercial storehouses of financial data (e.g., banks and insurance companies), ensuring that institutional perpetrators who abused their customers' data served appropriate sentences.[41]

In addition to assessing the costs of identity theft to consumers and corporations, Congress took note of identity crime because of its potential threat to national security. In the wake of the

---

35 18 U.S.C. § 1028A(a)(1). While the language of the aggravated identity theft provision is basically the same as that of the identity fraud provision, some courts have highlighted that the former covers a discrete list of particularly problematic federal felonies. *See, e.g.*, United States v. Ozuna-Cabrera, 663 F.3d 496, 499 (1st Cir. 2011) ("The statutes are [ ] distinguishable not by the method of procuring the means of identification, but by the underlying criminal conduct that they respectively target.").

36 *See* 18 U.S.C. § 1028A(b)(3). Specifically, the statute provides that in determining a term of imprisonment for the felony during which the perpetrator transferred, possessed, or used the means of identification, "a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section." 18 U.S.C. § 1028A(b)(3).

37 *See* Statement by President George W. Bush upon Signing H.R. 1731 (July 15, 2004), *as reprinted in* 2004 U.S.C.C.A.N. S15 ("Identity theft harms not only its direct victims but also many businesses and customers whose confidence is shaken. Like other forms of stealing, identity theft leaves the victim poor and feeling terribly violated.").

38 Pub. L. No. 108-159, 117 Stat. 1952.

39 Pub. L. No. 108-159, 117 Stat. 1952, 1956.

40 Pub. L. No. 108-159, 117 Stat. 1952, 1955–57.

41 *See* 18 U.S.C. § 1028A(c)(8).

September 11 attacks, federal and state officials realized that terrorist organizations were increasingly employing stolen and fabricated identities to evade detection by law enforcement.[42] Consequently, the aggravated identity theft provision also established a five-year sentencing enhancement for whoever "during and in relation to any [terrorism offense], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document."[43]

The ITPEA ultimately reflects the federal government's deep concern with the potential for high-stakes recidivism.[44] According to the relevant House Report, with just the ITADA in place, "many identity thieves receive[d] short terms of imprisonment or probation; after their release, many of these thieves [went] on to use false identities to commit much more serious crimes."[45] Congress attempted to address this issue with the mandatory sentencing enhancement in the aggravated identity theft provision, which "provides enhanced penalties for persons who steal identities to commit terrorist acts, immigration violations, firearms offenses, and other serious crimes."[46]

II. DIVERGENT APPROACHES AT THE CIRCUIT LEVEL

Earlier case law involving the ITPEA set the stage for the conflict that this Comment addresses. In *Flores-Figueroa v. United States*,[47] the Supreme Court held that the aggravated identity theft provision "requires the Government to show that the defendant knew that the 'means of identification' he or she unlawfully transferred, possessed, or used, in fact, belonged to 'another person.'"[48] The Court's holding was limited to clarifying the statute's mens rea requirement,[49] however, and did not address the scope of the term "uses." Thus, lower courts were left to

---

42 *See* H.R. REP. NO. 108-528, at 4, *as reprinted in* 2004 U.S.C.C.A.N. 779, 780.

43 18 U.S.C. § 1028A(a)(2).

44 *Cf.* Statement by President George W. Bush upon Signing H.R. 1731, *supra* note 37 ("The bill I'm about to sign sends a clear message that a person who violates another's financial privacy will be punished. . . . It reflects our Government's resolve to answer serious offenses with serious penalties.").

45 H.R. REP. NO. 108-528, at 3, *as reprinted in* 2004 U.S.C.C.A.N. 779, 779.

46 *Id.*

47 556 U.S. 646 (2009).

48 *Id.* at 647 (emphasis omitted).

49 Shortly after the Supreme Court clarified this heightened mens rea requirement, there was an influx of student pieces that investigated the Court's decision as it related to immigration reform. *See generally, e.g.*, Sean C.H. Flood, Note, *Of I.C.E. and* Mens Rea*:*

determine whether the aggravated identity theft provision applies to merely identity theft or to all identity fraud. This Comment defines identity *theft* as stealing the identity of another person and directly impersonating that person and identity *fraud* as generally misusing another's means of identification in the facilitation of fraud, which includes identity theft.

Circuits are split over whether the aggravated identity theft provision requires identity theft or merely identity fraud. First, and principally, circuits have disagreed about whether the term "uses" in the aggravated identity theft provision is ambiguous and whether the rule of lenity should consequently apply to narrow the statute's reach to cover only direct impersonation. Second, the circuits disagree about whether the provision's reference to the use of the means of identification of "another person" requires that the defendant steal the personal information from the victim. In other words, they disagree about whether the phrase refers exclusively to someone who has not consented to the use of the information.

A. Ambiguity of the Term "Uses"

1. Minority interpretation: impersonation.

The Sixth, First, and Ninth Circuits have held that the term "uses" is ambiguous, thereby allowing courts to apply the rule of lenity and narrowly interpret the provision to cover only identity *theft*. Accordingly, for a defendant to "use" a means of identification of another person, the defendant must directly impersonate another person.

The Sixth Circuit first advanced this interpretation in *United States v. Miller*.[50] The criminal scheme in *Miller* centered on the purchase of a parcel of real estate as an investment property.[51] To buy the land, David Miller formed a limited liability company (LLC) and recruited investors for funding.[52] When Miller failed to raise the necessary amount, he obtained a loan from a bank and

Illegal Immigration and the Knowledge Requirement of the Identity Theft Penalty Enhancement Act, 58 DRAKE L. REV. 323 (2009); Matthew T. Hovey, Comment, *Oh, I'm Sorry, Did That Identity Belong to You? How Ignorance, Ambiguity, and Identity Theft Create Opportunity for Immigration Reform in the United States*, 54 VILL. L. REV. 369 (2009); John P. Wixted, Note, *Unknowing Thieves: Reforming the Legal Link Between Immigration and Identity Theft*, 41 RUTGERS L.J. 403 (2009).

50 734 F.3d 530 (6th Cir. 2013).

51 *Id.* at 534.

52 *Id.*

pledged the property that the LLC sought to acquire as collateral.[53] To do so, however, Miller falsely represented that all the named investors were present at a meeting and unanimously voted to pledge the property as collateral.[54] Although Miller did not directly impersonate others—he simply misrepresented that they were present—the government argued that he used the investors' names when he "converted their names to his service" by saying that they did something that they in fact did not do.[55] Because the trial court found Miller guilty of the predicate felony of making false statements to a bank under 18 U.S.C. § 1028A(c)(4), the trial court also applied the aggravated identity theft provision to his sentence.[56]

The Sixth Circuit vacated his sentencing enhancement under the aggravated identity theft provision. Specifically, the Sixth Circuit held that the rule of lenity applied because there were "two reasonable interpretations of 'uses' and no conclusive guidance from the legislative history or case law."[57] The court first determined that the plain meaning of "use," as defined in dictionaries, is "'[t]o convert to one's service,' 'to employ,' 'to avail oneself of,' and 'carry out a purpose or action by means of.'"[58] Under this reading, Miller's misuse of the investors' names would fall into the generic "use" that the aggravated identity theft provision arguably criminalized.[59]

But the court also found support for Miller's position that, in this statutory context, "one 'uses' a person's name . . . only if one either passes himself off as that person or acts on behalf of that person."[60] Specifically, the court utilized the canons of noscitur a

---

53 *Id.*

54 *Id.* at 535.

55 *Miller*, 734 F.3d at 540.

56 *Id.* at 536.

57 *Id.* at 542; *see also id.* at 541–42 ("Unfortunately, there is nothing in the legislative history to indicate conclusively that Congress intended § 1028A to cover defendants falsely claiming that other individuals did things that they actually did not do. . . . [The relevant House Report] is brief and does not address the exact interpretive question presented.").

58 *Id.* at 540 (quoting Bailey v. United States, 516 U.S. 137, 145 (1995) (alteration in original)); *see also Use*, BLACK'S LAW DICTIONARY (6th ed. 1990).

59 *Miller*, 734 F.3d at 540. The government adopted this logic and conceded that, under this position, "if there is *any* false statement about authority, which necessarily involves the 'use' of someone's name, made in connection with a predicate offense under § 1028A(c), the government can *always* charge aggravated identity theft in addition to the underlying offense." *Id.* at 540–41 (emphasis in original) (quoting 18 U.S.C. § 1028A(a)(1)).

60 *Id.* at 541 (quoting 18 U.S.C. § 1028A(a)(1)). Miller further argued that his conduct did not constitute use of others' names because "he did not steal or possess their identities,

sociis[61] and ejusdem generis[62] to note that "the broad, dictionary definition of 'uses' is narrowed by its placement *near* and *after* 'transfers' and 'possesses,' both of which are specific kinds of use."[63] First, the noscitur a sociis canon suggested that the meaning of "uses" should draw from the meanings of the adjacent words "transfers" and "possesses." Second, the ejusdem generis canon meant that because "uses"—a general term—came after more specific verbs in statutory enumeration, "uses" should only embrace a meaning that is aligned with those of the preceding specific verbs.

Informed by these interpretive canons, the court reasoned that the term "uses" must have practical boundaries, especially in situations where the only means of identification at issue is a name.[64] In doing so, the court implied that there was merit in viewing impersonation as an aptly narrowed form of use in this particular context, though because Miller's case did not involve impersonation, the opinion did not provide further guidance on the matter.[65] Under this more limited reading, Miller did not "use" the investors' names by "merely lying about what they did."[66] Therefore, the Sixth Circuit—presented with two reasonable interpretations of "uses"—found the provision ambiguous, applied the rule of lenity, and resolved the matter in favor of Miller.[67]

The First Circuit found the reasoning in *Miller* persuasive. In *United States v. Berroa*,[68] the First Circuit analyzed the aggravated identity theft provision in the context of mail-fraud conspiracy. Berroa sought admission to practice medicine in Puerto Rico but failed to pass a required exam.[69] As a result, he enlisted the help of an employee of the Puerto Rico Board of Medical Examiners, who falsified passing test scores in his file.[70] When Berroa

impersonate them or pass himself off as one of them, act on their behalf, or obtain anything of value in one of their names." *Id.*

61 *See Noscitur a sociis*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("[T]he meaning of an unclear word or phrase . . . should be determined by the words immediately surrounding it.").

62 *See Ejusdem generis*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("[W]hen a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same class as those listed.").

63 *Miller*, 734 F.3d at 541 (emphasis in original) (quoting 18 U.S.C. § 1028A(a)(1)).

64 *See id.*

65 *See id.*

66 *Id.*

67 *Id.* at 542.

68 856 F.3d 141 (1st Cir. 2017).

69 *Id.* at 147.

70 *Id.* at 147–48.

entered medical practice as a doctor, he issued prescriptions to his patients.[71] As such, the government alleged that the use of patient names and addresses on the prescriptions for mail fraud under 18 U.S.C. § 1028A(c)(5) constituted use without lawful authority of the identification of another person because Berroa was not properly admitted to practice medicine and therefore could not lawfully issue prescriptions.[72]

The First Circuit vacated Berroa's convictions for aggravated identity theft, reasoning that legislative history supports a narrower interpretation of "uses."[73] As a preliminary matter, the First Circuit defined the rule of lenity as a rule of statutory construction that "requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them."[74] Looking to the text, the court found the statutory language ambiguous, recognizing that "'use' cannot be given its broadest possible meaning, which would subsume the separate statutory terms 'transfer[ ]' and 'possess[ ].'"[75] Looking to legislative history, however, the court noted that the government's broad interpretation "could encompass every instance of specified criminal misconduct in which the defendant speaks or writes a third party's name," thereby leading to "extreme result[s]" not intended by Congress.[76] Thus, the court gave considerable weight to legislative history and held in favor of a narrower reading of "uses." Accordingly, the court "read the term 'use' to require that the defendant attempt to pass him or herself off as another person or purport to take some other action on another person's behalf."[77]

The Ninth Circuit also falls into the minority camp. In *United States v. Hong*,[78] the Ninth Circuit analyzed the aggravated identity theft provision as applied to health-care fraud. Hong owned and operated three massage and acupuncture clinics in Southern California.[79] He made an arrangement with physical-therapy companies under which he would amass a set of customers, tell those customers that Medicare would cover the costs of massage and acupuncture sessions, and—with the customers' consent—

---

71 *Id.* at 155.
72 *Id.*
73 *See Berroa*, 856 F.3d at 155–56, 157 n.8.
74 *Id.* at 157 n.8 (quoting United States v. Gray, 780 F.3d 458, 468 (1st Cir. 2015)).
75 *Id.* at 156 (alterations in original) (quoting 18 U.S.C. § 1028A(a)(1)).
76 *Id.*
77 *Id.* at 156–57.
78 938 F.3d 1040 (9th Cir. 2019).
79 *Id.* at 1044.

share their Medicare information with the companies.[80] The companies had Medicare provider numbers that allowed them to submit claims for payments, notwithstanding the fact that Medicare usually does not cover massages or acupuncture.[81] The parties agreed that Hong would supply a clinic, while the companies would bill Medicare for physical-therapy services that, in reality, were massage and acupuncture sessions.[82] At trial, the jury returned a guilty verdict on all counts, including two counts of aggravated identity theft.[83]

The Ninth Circuit reversed. Specifically, the Ninth Circuit held that the rule of lenity applied and that Hong "did not 'use' [others'] identities within the meaning of the aggravated identity theft statute."[84] The court focused on the fact that Hong provided massage services to patients to treat their pain and then misrepresented those treatments as Medicare-eligible physical-therapy services.[85] Therefore, the court concluded that, while Hong and his accomplices' conduct ran afoul of other statutes, they did not attempt to "pass themselves off as [others]."[86] This succinct statement from the Ninth Circuit aptly summarizes the minority interpretation of the aggravated identity theft provision.

2. Majority interpretation: general misuse.

The Fifth, Fourth, D.C., Eleventh, and Eighth Circuits, on the other hand, have held that the term "uses" is not ambiguous. They therefore do not apply the rule of lenity, and consequently interpret the provision's meaning broadly. Accordingly, for a defendant to use a means of identification of another person, the defendant need only generally misuse another's information in the facilitation of fraud. This interpretation includes conduct beyond direct impersonation.

The Fifth Circuit concisely spelled out this interpretation in *United States v. Mahmood*.[87] Mahmood was a licensed physician

---

80 *Id.*

81 *Id.*

82 *Id.* ("When therapists asked Hong about providing patients with [actual] physical therapy, Hong told them [that] the patients prefer massages and might stop coming to the clinics if made to exercise.").

83 *Hong*, 938 F.3d at 1045.

84 *Id.* at 1051.

85 *Id.*

86 *Id.* (quoting *Berroa*, 856 F.3d at 156).

87 820 F.3d 177 (5th Cir. 2016).

who owned a number of hospitals in Texas.[88] He committed health-care fraud by secretly altering Medicare reimbursement claims: he replaced patients' basic primary diagnoses with their more complex secondary diagnoses, which resulted in $143,608 in overpayments .[89] He did not directly impersonate the patients but rather used their means of identification in perpetuating a fraud scheme.

Still, the Fifth Circuit held that the provision "d[id] not require actual theft or misappropriation of a person's means of identification as an element of aggravated identity theft."[90] The court reasoned that the provision was unambiguous and that it "plainly criminalizes situations where a defendant gains lawful possession of a person's means of identification but proceeds to use that identification unlawfully and beyond the scope of permission granted."[91] Unlike the courts that subscribe to the minority position, the Fifth Circuit stated that because of the weight of the plain meaning of the provision, it need not resort to traditional canons of statutory interpretation or legislative history to discern Congress's intent.[92] Put another way, while the minority and majority positions arrive at similar conclusions regarding the plain meaning of the word "uses," the majority approach does not perceive the provision as blurring the word's plain meaning and therefore does not rely on other interpretive considerations.

The Fourth Circuit set forth a similar position in *United States v. Abdelshafi*.[93] In *Abdelshafi*, the Fourth Circuit applied the aggravated identity theft provision in the context of health-care fraud. Mohamed Abdelshafi operated a third-party vendor for medical transportation services and contracted with a health maintenance organization (HMO) to drive Medicaid patients to and from health facilities in Virginia.[94] The HMO gave Abdelshafi a daily log with patients' Medicaid identification numbers and trip details.[95] Abdelshafi used the personal information on the claim forms to charge the HMO for trips that did not occur and fraudulently overbilled the HMO by over $300,000.[96] The trial

---

88 *Id.* at 182.
89 *See id.* at 184.
90 *Id.* at 187.
91 *Id.* at 187–88.
92 *Mahmood*, 820 F.3d at 188.
93 592 F.3d 602 (4th Cir. 2010).
94 *Id.* at 605.
95 *Id.*
96 *Id.*

court convicted Abdelshafi on fifteen counts of health-care fraud and two counts of aggravated identity theft.[97]

The Fourth Circuit affirmed and, through a plain meaning analysis, held that the aggravated identity theft provision unambiguously "prohibit[ed] an individual's knowing use of another person's identifying information without a form of authorization recognized by law."[98] The court reasoned that while Abdelshafi "had authority to possess the [identifying information], he had no authority to use [it] unlawfully so as to perpetuate a fraud."[99] In addition, the court rejected Abdelshafi's policy argument that every instance of health-care fraud related to provider payments would constitute aggravated identity theft.[100] That this sliver of health-care fraud—which implicated individuals' privacy and security interests in medical services and thus justified increased punishment—would always fall within the statute's scope was "not particularly noteworthy" to the court.[101] Thus, the court "decline[d] to narrow the application of § 1028A(a)(1) to cases in which an individual's identity has been misrepresented."[102]

The D.C. Circuit arrived at a similar conclusion in *United States v. Reynolds*.[103] Reynolds was the chief financial officer of a church and swindled the institution out of more than $850,000.[104] He extended the church's line of credit at a bank by copying and pasting church officers' digital signatures, to which he had access, to create false increased-borrowing approval letters.[105] The trial court found Reynolds guilty of bank fraud and aggravated identity theft, among other violations.[106]

The D.C. Circuit affirmed and held that "the statute [was] clear" and that the phrase "'use[ ] . . . without lawful authority' easily encompasse[d] situations in which a defendant gains access

---

97 *Id.* at 604.

98 *Abdelshafi*, 592 F.3d at 609.

99 *Id.* (emphasis omitted).

100 *Id.* at 609–10 ("We adhere to the principle that '[f]ederal crimes are defined by Congress, and so long as Congress acts within its constitutional power in enacting a criminal statute, this Court must give effect to Congress' expressed intention concerning the scope of conduct prohibited.'" (quoting United States v. Kozminski, 487 U.S. 931, 939 (1988) (alteration in original))).

101 *Id.* at 609.

102 *Id.*

103 710 F.3d 434 (D.C. Cir. 2013).

104 *Id.* at 435.

105 *Id.*

106 *Id.*

to identity information legitimately but then uses it illegitimately—in excess of the authority granted."[107] The court explicitly rejected Reynolds's argument that "use" in the provision requires the stealing of information, accepting that because "[t]he statutory text [was] unambiguous," other interpretive tools like legislative history could not be used to support his argument.[108] The court's decision made no mention of impersonation, perhaps as a consequence of never reaching the question of if Reynolds "stole" the church officer's identity information.[109] In other words, it did not matter that Reynolds did not directly impersonate the church officers by assuming their identities or stepping in their shoes; digitally fabricating their approval of the transactions was enough to qualify as a "use" of identity information. The outcome of this case contrasts with that in *Miller*, which involved a similar set of facts regarding representations and authorization.

The Eleventh Circuit adopted the reasoning of *Reynolds* in *United States v. Munksgard*.[110] Matthew Munksgard knowingly made a false statement to obtain a loan from a bank insured by the Federal Deposit Insurance Corporation.[111] In doing so, "he forged another person's name to a surveying contract that he submitted to a bank in support of his loan application."[112] The court transparently teed up both the issue at hand and its stance on the matter:

> The question before us is whether Munksgard's conduct qualifies as a prohibited "use[ ]" within the meaning of § 1028A(a)(1). Munksgard insists that we should cabin the meaning of "use[ ]" to crimes in which the accused attempted to impersonate, or act "on behalf of," someone else. We disagree. Plain meaning, statutory context, and existing precedent all show that Munksgard "use[d]" his victim's means of identification when he employed that person's signature to obtain the loan and thereby converted the signature to his own service.[113]

---

[107] *Id.* at 436 (alterations in original) (quoting 18 U.S.C. § 1028A(a)(1)).

[108] *Reynolds*, 710 F.3d at 436.

[109] *Id.* at 435–36 (declining to determine whether Reynolds stole identity information because it was unnecessary based on the plain meaning of the statute).

[110] 913 F.3d 1327 (11th Cir. 2019).

[111] *Id.* at 1329.

[112] *Id.* at 1330.

[113] *Id.* (alterations in original) (quoting 18 U.S.C. § 1028A(a)(1)).

The court also reasoned that "use" in other criminal statutes supported the plain language reading that the term entails "employing or converting an object to one's service."[114] Like in *Reynolds*, the court here implicitly suggested that Munksgard had not directly impersonated the other person when forging his name because he had not held himself out as that person to another entity; rather, he had fabricated approval of the transaction. Nonetheless, the Eleventh Circuit found that the provision's cross references to 18 U.S.C. § 1028A(c) supported a more expansive reading of the term "uses."[115]

The Eighth Circuit took a stronger stance against the application of the rule of lenity in *United States v. Gatwas*.[116] Lony Gatwas was a Des Moines tax agent who prepared personal income tax returns for his clients that "obtained inflated refunds by falsely claiming dependents, including returns that reported several of Gatwas's eight children as dependents of his clients."[117] The trial court sentenced him to forty-five months for wire and tax fraud as well as aggravated identity theft.[118] On appeal, Gatwas argued that the trial court erred because the aggravated identity theft provision "requires proof that he stole or assumed the identity of another person."[119]

The Eighth Circuit "reject[ed] Gatwas's argument that the statute [was] ambiguous and the rule of lenity therefore applie[d]."[120] In doing so, the court observed that multiple prior decisions in its sister circuits had "upheld [aggravated identity theft] convictions where the defendant neither stole nor assumed the identity of [ ] [an]other person."[121] Furthermore, the court noted that many of its sister circuits had "construed the word 'use[s]' broadly, relying on the statute's causation element—that

---

114 *Id.* at 1335 (citing opinions that more broadly define the term "use" in the context of 18 U.S.C. § 924(c)(1)(A), 18 U.S.C. § 922(g)(9), 18 U.S.C. § 2701(c)(2), and U.S.S.G. § 3B1.4).

115 *Munksgard*, 913 F.3d at 1335 ("While these references may not foreclose an impersonation-based 'on behalf of' reading, they also don't preclude—and on balance, we think they support—an interpretation of 'use[ ]' that more broadly forbids one from 'employ[ing]' or 'convert[ing] to [his] service' another's name." (alterations in original) (quoting *Use*, WEBSTER'S NEW INTERNATIONAL DICTIONARY (2d ed. 1944))).

116 910 F.3d 362 (8th Cir. 2018).

117 *Id.* at 364.

118 *Id.*

119 *Id.*

120 *Id.* at 368 n.2.

121 *Gatwas*, 910 F.3d at 365 (first citing United States v. White, 846 F.3d 170, 177–78 (6th Cir. 2017); then citing *Reynolds*, 710 F.3d at 435–36; and then citing United States v. Dvorak, 617 F.3d 1017, 1024–27 (8th Cir. 2010)).

the use be during and in relation to an enumerated felony—to limit its scope."[122] Therefore, the court reasoned that circuit case law made clear that "no 'grievous ambiguity or uncertainty' in the statute warrant[ed] application of the rule of lenity in this case."[123]

B. Significance of the Owner's Consent

A related but distinct issue is whether the use of the means of identification of "another person" requires the defendant to have stolen the personal information from the victim. That is, the circuits disagree over whether the phrase refers exclusively to an owner who did not consent to said use.

The Seventh Circuit is the sole proponent of the minority interpretation. Specifically, in *United States v. Spears*,[124] the court reviewed the convictions of a defendant who was in the business of selling counterfeit credentials such as handgun permits and drivers' licenses.[125] The court reversed the conviction under the aggravated identity theft provision:

> "[A]nother person" is ambiguous: neither text nor context tells us whether "another" means "person other than the defendant" or "person who did not consent to the information's use." That § 1028A deals with identity *theft* helps resolve the ambiguity in favor of the latter understanding, while reading "another person" to mean "person other than the defendant" treats § 1028A as forbidding document counterfeiting and other forms of fraud, a crime distinct from theft.

In other words, the court held that the provision "uses 'another person' to refer to a person who did not consent to the use of the 'means of identification.'"[126] In this case, "[p]roviding a client with a bogus credential containing the client's own information is identity *fraud* but not identity *theft*; no one's identity has been stolen

---

[122] *Id.* (first citing United States v. Michael, 882 F.3d 624, 628 (6th Cir. 2018) ("The salient point is whether the defendant used the means of identification to further or facilitate the . . . fraud."); and then citing United States v. Otuya, 720 F.3d 183, 189 (4th Cir. 2013) ("[A] defendant who uses the means of identification of another 'during and in relation to any felony violation enumerated' in the statute necessarily lacks a form of authorization recognized by law.")).

[123] *Id.* at 368 n.2 (quoting Muscarello v. United States, 524 U.S. 125, 138–39 (1998)).

[124] 729 F.3d 753 (7th Cir. 2013).

[125] *Id.* at 754.

[126] *Id.* at 758.

or misappropriated."[127] Accordingly, for a defendant to use a means of identification of "another person" under the Seventh Circuit's interpretation, the defendant must steal the information from the victim.

In contrast, the Ninth, Eighth, and Fourth Circuits have held that "another person" does not exclusively refer to an owner who did not consent to said use. Accordingly, for a defendant to use a means of identification of "another person," the defendant need not have stolen the information.

In *United States v. Osuna-Alvarez*,[128] the Ninth Circuit held that, under a plain meaning analysis, "regardless of whether the means of identification was stolen or obtained with the knowledge and consent of its owner, the illegal use of the means of identification alone violates § 1028A."[129] Moreover, in *United States v. Hines*,[130] the Eighth Circuit held that a defendant acts unlawfully regardless of whether the defendant has used another's name without permission or has obtained consent, emphasizing that consent is not pertinent to the inquiry of whether the perpetrator used the name in connection to a predicate felony.[131] In addition, in *United States v. Otuya*,[132] the Fourth Circuit held that "one does not have 'lawful authority' to consent to the commission of an unlawful act. Nor does a 'means of identification' have to be illicitly procured for it to be used 'without lawful authority.'"[133] While the significance of the owner's consent is not the focal point of this Comment, it has important implications for how courts should interpret the aggravated identity theft provision in more modern, technological contexts.

III. INTERPRETING THE AGGRAVATED IDENTITY THEFT PROVISION

This Part uses interpretive tools to determine how to apply the aggravated identity theft provision. Part III.A employs textual analysis and also examines *Smith*, an analogous case that

---

127 *Id.* at 756.

128 788 F.3d 1183 (9th Cir. 2015) (per curiam).

129 *Id.* at 1185–86.

130 472 F.3d 1038 (8th Cir. 2007) (per curiam), *abrogated on other grounds by* Flores-Figueroa v. United States, 556 U.S. 646 (2009).

131 *See id.* at 1040.

132 720 F.3d 183 (4th Cir. 2013).

133 *Id.* at 189 (quoting 18 U.S.C. § 1028A(a)(1)).

wrangled with statutory language similar to the aggravated identity theft provision. In general, courts assessing terminology in similar statutory contexts have also focused on the broad ordinary meaning of the term "uses." This helps to clarify the discrepancies between the minority and majority camps with respect to textual interpretation. In addition, the surplusage canon counters the canons of noscitur a sociis and ejusdem generis, granting "uses" a different meaning to avoid duplicating the meaning of the other two verbs in the statute.

The remaining Sections use additional materials to expand on these points. Part III.B draws on the House Report and amendment notes to the ITPEA, explaining that the specific references to identity fraud and identity theft in legislative history and statutory context mean that Congress did not intend to limit the aggravated identity theft provision to only cases of identity theft and direct impersonation. Moreover, as a matter of policy, the fact that the aggravated identity theft provision enumerates specific categories of predicate felonies quells the concern that a broad reading of the provision would result in its application to situations beyond which Congress had originally considered while drafting the ITADA and the ITPEA. Part III.C then argues that the application of the rule of lenity is improper in the context of the aggravated identity theft provision.

A. Textual Interpretation

1. The plain meaning of "uses."

In approaching this issue from a textual perspective, it is helpful to further examine the four decisions from Part II.A.1 that emphasized the ordinary meaning and dictionary definition of "uses" in the aggravated identity theft provision. As a preliminary matter, the Supreme Court has recognized that the term "'use[s]' poses some interpretational difficulties because of the different meanings attributable to it."[134] It is unsurprising, then, that while the four cases all arrive at comparable conclusions when analyzing the term in isolation, they subsequently diverge on the interpretive strength of the plain meaning vis-à-vis the statutory context. Predictably, this divide falls in line with whether the courts subscribe to the impersonation or general-misuse interpretation.

---

[134] Bailey v. United States, 516 U.S. 137, 143 (1995).

Circuits in the impersonation camp have sought to balance the plain meaning with statutory context. For example, in *Miller*, the Sixth Circuit stated that, "[d]efined in isolation from its statutory context, the dictionary meaning of the word 'use' is '"[t]o convert to one's service," "to employ," "to avail oneself of," and "to carry out a purpose or action by means of."'"[135] Nonetheless, the court went on to explain that the "meaning of statutory language, plain or not, depends on context," ultimately holding that the context of the aggravated identity theft provision produced two equally reasonable interpretations of "uses."[136] Similarly, in *Berroa*, the First Circuit noted that the "statute at issue here fail[ed] to provide a specific definition" for "use" and outlined the risks associated with giving the term its broadest possible meaning.[137]

In contrast, circuits in the general-misuse camp have been more comfortable allowing the plain meaning to speak for itself. For example, in *Abdelshafi*, the Fourth Circuit observed that the Supreme Court previously indicated in its discussion of § 1028A(a)(1) in *Flores-Figueroa* that "[n]o special context is present here."[138] Accordingly, its analysis "focuse[d] on the statute's plain text."[139] Similarly, in *Munksgard*, the Eleventh Circuit assessed the definitions of the verb "use" in both standard English-language dictionaries and legal dictionaries, ultimately concluding that the term "does not bear some idiosyncratic connotation in the legal context."[140] Using these two types of dictionaries, the Eleventh Circuit determined that the definitions stating "[to] take, hold, or deploy (something) as a means of accomplishing or achieving something,"[141] as well as "[t]o employ for the accomplishment of some purpose"[142] supported its argument that impersonation is not necessary.

Turning to an analogous case that has wrangled with similar statutory language helps this analysis. In *Smith*, the Supreme Court faced a similar issue when interpreting 18 U.S.C. § 924, which criminalizes and establishes a minimum sentence for the

---

135 *Miller*, 734 F.3d at 540 (quoting *Bailey*, 516 U.S. at 145 (alteration in original)).

136 *Id.* at 540–41 (quoting *Bailey*, 516 U.S. at 145).

137 *See Berroa*, 856 F.3d at 156.

138 *Abdelshafi*, 592 F.3d at 607 (quoting *Flores-Figueroa*, 556 U.S. at 652 (alteration in original)).

139 *Id.*

140 *Munksgard*, 913 F.3d at 1334.

141 *Id.* (quoting *Use*, OXFORD DICTIONARY OF ENGLISH (3d ed. 2010)).

142 *Id.* (quoting *Use*, BLACK'S LAW DICTIONARY (10th ed. 2014) (alteration in original)).

"use[ ]" of a firearm "during and in relation to any crime of violence or drug trafficking crime."[143] The Court examined whether the exchange of a gun for narcotics constituted "use" of a firearm during and in relation to a drug-trafficking crime within the meaning of the statute.[144] The petitioner argued that the penalty for using a firearm during and in relation to a drug-trafficking offense covered only situations in which the firearm was used as a weapon.[145] That is, the petitioner argued that the provision "d[id] not extend to defendants who use[d] a firearm solely as a medium of exchange or for barter."[146]

The Court ruled against the petitioner and held that "using a firearm in a guns-for-drugs trade may constitute 'us[ing] a firearm' within the meaning of § 924(c)(1)."[147] Specifically, the Court examined the following before arriving at its conclusion: (1) the broad ordinary meaning of "use," (2) the United States Sentencing Commission Guidelines Manual, and (3) the remaining terminology present in § 924(c)(1).[148] *Smith* confirms the availability of an unambiguously expansive notion of "use" in a criminal context and therefore strongly supports a more expansive view of the term "uses" in the analogous aggravated identity theft context.[149]

The ruling in *Smith* is comparable and is, at least plausibly, a reflection on the Court's approach to textual interpretation. It is also worth noting, however, that the dissenting opinion in *Smith* argued that "[t]o use an instrumentality ordinarily means to use it for its intended purpose" and provided an example:

---

143 18 U.S.C. § 924(c)(1)(A).

144 *See Smith*, 508 U.S. at 227–37.

145 *Id.* at 227.

146 *Id.*

147 *Id.* at 237 (alteration in original).

148 *See id.* at 228–34.

149 In *Bailey v. United States*, however, the Court limited the reach of this view by interpreting that § 924(c)(1) required "active employment" of the firearm by a defendant—that is, "a use that makes the firearm an *operative factor* in relation to the predicate offense." *Bailey*, 516 U.S. at 143 (emphasis added). Thus, the Court implicitly overruled *Smith* in this regard, with the sentiments in *Bailey* falling in line with those from Scalia's dissent in *Smith* (discussed above). Nonetheless, *Bailey* still leads to an expansive notion of "use" in the context of aggravated identity theft. The use of personal information in an identity fraud scheme, regardless of whether said use involves impersonation, is always an "operative factor" in relation to carrying out the predicate offense. In other words, active employment of personal information does not necessarily nor exclusively implicate impersonation; personal information in an identity fraud scheme is inherently central in furthering a perpetrator's goals, notwithstanding specific methods of use (i.e., impersonation versus general use).

> When someone asks, "Do you use a cane?," he is not inquiring whether you have your grandfather's silver-handled walking stick on display in the hall; he wants to know whether you *walk* with a cane. Similarly, to speak of "using a firearm" is to speak of using it for its distinctive purpose, *i.e.*, as a weapon.[150]

This argument is reminiscent of the arguments from the impersonation camp that posit that the aggravated identity theft provision inherently requires that the defendant have impersonated another person. The resultant ambiguity stems from whether the use of a means of identification necessarily entails the assumption or misappropriation of the identity itself for its "intended purpose." In other words, one could reasonably argue that the use of a means of identification to generally facilitate fraud is not the most natural meaning of identity theft.

Despite this competing perspective, the majority's analysis in *Smith*, combined with other tools of construction, ultimately supports an argument that the provision is not grievously ambiguous and that the language at hand cuts in favor of a broader interpretation. Still, the ideas in the dissent suggest that the analysis should not stop here. Thus, while *Smith* does not definitively resolve the circuit split, the Court's approach to "uses" markedly tips the scales in favor of the majority's broad approach to the aggravated identity theft provision.

2. Interpretive canons and (con)textual tiebreakers.

When plain and ordinary meaning analyses are potentially inconclusive, judges often turn to canons of statutory interpretation to help discern meaning. In the case of the aggravated identity theft provision, the canon of surplusage is particularly useful. Under the surplusage canon, courts should "give effect, if possible, to every clause and word of a statute" in a way that "no clause, sentence, or word shall be superfluous, void, or insignificant."[151] As a preliminary matter, Black's Law Dictionary defines "trans-

---

[150] *Smith*, 508 U.S. at 242 (Scalia, J., dissenting) (emphasis in original).

[151] Duncan v. Walker, 533 U.S. 167, 174 (2001) (first quoting United States v. Menasche, 348 U.S. 528, 538–39 (1955); and then quoting Market Co. v. Hoffman, 101 U.S. 112, 115 (1879)).

fer" as "[t]o convey or remove from one place or one person to another," or "to change over the possession or control of,"[152] while the definition of "possess" is "[t]o have in one's actual control."[153]

To give full effect to "uses" and to avoid duplicating the meaning of the other terms, "uses" should take on a definition that captures all of the *remaining* concepts not addressed by the preceding terms. In a strict sense, "transfers" and "possesses" are types of use and thereby necessarily implicate "uses." As such, the explicit distinction between "transfers," "possesses," and "uses" cuts in favor of granting "uses" a meaning that expands beyond that of its two companion verbs so as to avoid overlapping denotations. In effect, limiting "uses" to direct impersonation restricts the term to a definition that is already captured in "transfers" and "possesses." Specifically, direct impersonation involves a *transfer* of a means of identification from the victim to the impersonator and the impersonator's *possession* of those means. This nexus of victim-to-impersonator transfer and direct exchange of control, however, is not always present in the general-misuse cases that courts in the majority camp discuss. Put another way, the idea of direct impersonation is already covered by the preceding terms, so "uses" must go beyond this existent realm of coverage to include more general use in crime facilitation.

The surplusage canon mitigates the Sixth Circuit's concern in *Miller* that without the canons of noscitur a sociis and ejusdem generis, there would be no limiting principle to the interpretation of "uses." Recall that in *Miller* the court employed two particular canons to interpret the aggravated identity theft provision. First, it applied the canon of noscitur a sociis, which instructs that "the meaning of an unclear word or phrase . . . should be determined by the words immediately surrounding it."[154] Second, it applied the canon of ejusdem generis, which instructs that "when a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same class as those listed."[155]

The Sixth Circuit in *Miller* reasoned that the principles of noscitur a sociis and ejusdem generis supported a narrower notion of the provision, but it failed to consider the implications of surplusage. The court noted that "the broad, dictionary definition

---

[152] *Transfer*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[153] *Possess*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[154] *Noscitur a sociis*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[155] *Ejusdem generis*, BLACK'S LAW DICTIONARY (11th ed. 2019).

of 'uses' is narrowed by its placement *near* and *after* 'transfers' and 'possesses,' both of which are specific kinds of use."[156] Therefore, the defendant "persuasively argue[d] that . . . 'uses' is not as expansive as the government suggest[ed] and that the term must have practical boundaries."[157] Overall, the tension between the canon of surplusage and those employed by the Sixth Circuit highlights the "back-and-forth" of competing canons that can occur during statutory interpretation.[158]

On balance, however, it should not necessarily follow that the commonalities between the verbs "transfer," "possess," and "use" necessarily result in a definitional restriction. This is because the surplusage canon, when assessed alongside legislative context, leads to a more tenable outcome. Considering the historical development of the ITADA and the ITPEA and the issues posed by the Information Age, it is likely that Congress intended "uses" to capture actions far beyond unlawful transfers and possessions of another person's identifying information,[159] advancing a reading under the surplusage canon. Recognizing that rising technologies would facilitate more identity crimes through complex fraud schemes, Congress sought ways to combat the plethora of new risks that went beyond traditional "dumpster diving" identity theft and, implicitly, classical instances of direct impersonation.[160] When read alongside interpretive canons, this history pairs the best with the surplusage canon and is more hostile to canons that would narrow the scope of coverage of the proscribed behavior for a statute passed when new opportunities for identity crime were rapidly increasing. In this way, legislative history and intent break the tie between the competing canons: the surplusage canon leads to a broader reading while the canons employed by the Sixth Circuit lead to a narrower result, but legislative considerations counsel that the former is a more harmonizing point of view.

---

156 *Miller*, 734 F.3d at 541 (emphasis in original).

157 *Id.*

158 *See* Stephen Ferro, Comment, *It's All About (Re)location: Interpreting the Federal Sentencing Enhancement for Relocating a Fraudulent Scheme*, 88 U. CHI. L. REV. 1465, 1492 (2021) (explaining Professor Karl Llewellyn's criticism that "there are two opposing canons on almost every point" (quoting Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395, 401 (1950))).

159 *Cf.* H.R. REP. NO. 108-528, at 4–5, *as reprinted in* 2004 U.S.C.C.A.N. 779, 780–81 (providing examples of how information originally gathered for authorized purposes can be stolen through hacking and other technological means).

160 *See id.*

With that said, the surplusage canon also quells auxiliary issues arising under the title-and-headings canon. Under this interpretive principle, a legislative act's titles and headings are all "useful navigational aids"[161] and "'tools available for the resolution of a doubt' about the meaning of a statute."[162] The official title associated with the identity fraud provision of the ITADA is "Fraud and related activity in connection with identification documents, authentication features, and information."[163] The official title associated with its ITPEA counterpart, the aggravated identity theft provision, is "Aggravated identity theft."[164]

In this situation, one could initially argue that the differences between the titles of the identity fraud provision and the aggravated identity theft provision suggest an underlying conceptual divide between fraud (i.e., generally misusing a person's identity) and theft (i.e., impersonating another person). Thus, if a court were to find the respective titles determinative, the meaning of "use" in the latter statute would likely align with a more traditional understanding of theft. According to this premise, the title-and-headings canon would cut in favor of the impersonation camp. However, other factors suggest that this cannot be the case. The statute itself already includes the terms "transfers" and "possesses," so to read the title as limiting the statute to only impersonation would conflict with its very content. Furthermore, it is commonplace in Supreme Court jurisprudence that titles and headings generally will not be dispositive where there are more easily discernible indicators of meaning.[165] With the cogent textual interpretation above, the title-and-headings canon fails to overcome this presumption and—like noscitur a sociis and ejusdem generis—cannot compete against the surplusage canon and the clear implications of legislative history.

---

[161] ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 221 (2012).

[162] Almendarez-Torres v. United States, 523 U.S. 224, 234 (1998) (quoting Brotherhood of R.R. Trainmen v. Balt. & Ohio R.R., 331 U.S. 519, 528–29 (1947)).

[163] 18 U.S.C. § 1028.

[164] 18 U.S.C. § 1028A.

[165] *See, e.g.*, *Brotherhood of R.R. Trainmen*, 331 U.S. at 528 ("[H]eadings and titles are not meant to take the place of the detailed provisions of the text."); Yates v. United States, 574 U.S. 528, 552 (2015) (Alito, J., concurring) ("Titles, of course, are [ ] not dispositive.").

B. The Amendment Notes to the ITPEA

The textual analysis above demonstrates that the plain meaning of "uses" cuts in favor of a broader interpretation of the aggravated identity theft provision. The analysis also leads to two additional observations. First, Congress used both the terms "identity fraud" and "identity theft" in reports and commentary. Some may argue that the surface-level distinction means that the aggravated identity theft provision should only cover impersonation, not general misuse. However, Congress likely used these terms to refer more broadly to the use of personal information to facilitate or perpetuate fraud given the language of the House Report and amendment notes to the ITPEA. Accordingly, the facial differentiation between the terms "identity fraud" and "identity theft" in the titles has little bearing.

Second, the fact that the aggravated identity theft provision imposes a mandatory penalty enhancement provides a helpful clue regarding congressional intent. The mandatory minimum sentencing associated with the aggravated identity theft provision reflects Congress's concern with high-stakes identity theft recidivism as well as its ambivalence toward the consistent application of the Federal Sentencing Guidelines. This suggests that Congress intended for the provision to cover instances of identity crime beyond impersonation in order to have sufficient deterrent effects in an increasingly digital environment.

1. References to identity fraud and theft.

Thus far, the ambiguity between identity fraud and identity theft has been lurking underneath this line of analysis. In *Flores-Figueroa*, the Supreme Court noted in a slightly different context that identity fraud focuses on the "use of a false ID" while identity theft focuses on the "use of an ID belonging to someone else."[166] The Court observed that Congress might have meant for the statute to cover only identity theft by "separat[ing] the fraud crime from the theft crime in the statute itself."[167] However, the Court also speculated that Congress might have meant for the statute to cover both identity theft and fraud by equating the terms in legislative documents.[168]

---

166 *Flores-Figueroa*, 556 U.S. at 655.

167 *Id.*

168 *Id.*

The House Report and amendment notes to the ITPEA provide useful information on the matter. Critically, the first sentence of the statement of purpose for the ITPEA states only that the Act "addresses the growing problem of identity theft."[169] In later sections, however, the House Report refers to the fact that the legislation addresses both identity fraud and identity theft without distinguishing between the two. For example, it explicitly states that "[t]he terms 'identity theft' and 'identity fraud' refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic or other gain, including immigration benefits."[170] In addition, the chairman of the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security expressed that "[i]dentity theft and identity fraud are terms used to refer to all types of crimes in which an individual's personal or financial data is misused, typically for economic gain or to facilitate another criminal activity."[171]

Given these assertions, Congress used the initial phrase "identity theft" as a signal to include the traditional notions of both theft and fraud. More specifically, Congress used the initial phrase to refer to the use of personal information both to impersonate another and to facilitate fraud. In other words, Congress likely attributed the technical definition of identity fraud to identity theft in the statement of purpose. This effaces the differences between the titles of the identity fraud provision and the aggravated identity theft provision, minimizing the residual challenge that the title-and-headings canon poses to a more expansive notion of theft.

That being said, other portions of the House Report shed additional light on Congress's conceptualization of identity theft. In particular, Congress expressed its concern that "many perpetrators of identity theft receive[d] little or no prison time."[172] It believed that the minimal severity of punishment became a "tacit encouragement to those arrested to continue to pursue such

---

169 H.R. REP. NO. 108-528, at 3, *as reprinted in* 2004 U.S.C.C.A.N. 779, 779.

170 *Id.* at 4, *as reprinted in* 2004 U.S.C.C.A.N. 779, 780.

171 *Identity Theft Penalty Enhancement Act, and the Identity Theft Investigation and Prosecution Act of 2003: Hearing on H.R. 1731 and H.R. 3693 Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 108th Cong. 1 (2004) (statement of Rep. Howard Coble, Chairman, Subcomm. on Crime, Terrorism, and Homeland Sec.).

172 H.R. REP. NO. 108-528, at 5, *as reprinted in* 2004 U.S.C.C.A.N. 779, 781.

crimes."[173] Congress then presented eight examples of these situations, each of which were examples of more traditional, restrictive notions of identity theft that involved direct impersonation. For example, they included the following story:

> William K. Maxfield used the Social Security number of a William E. Maxfield (no relation) to obtain loans and lines of credit. He was able to obtain the false Social Security number through his employment at an auto dealership. Maxfield defaulted on some of the loans but was timely on others. Ultimately, most of the lenders were paid; however, the more significant injury was to William E. Maxfield, who suffered harm to his credit rating and had great difficulty in clearing what appeared to be delinquent accounts. On January 9, 2003, William K. Maxfield was sentenced to 10 months imprisonment.[174]

Courts that have weighed in on the matter have generally commented that all eight examples primarily involve the defendant's impersonation of the victim.[175] Put another way, none of the examples describe instances of general misuse of personal information.

However, the fact that the eight examples in the House Report primarily involve impersonation does not affect the outcome of this analysis for two main reasons. First, in the preceding paragraphs, Congress described how "identity thieves" were gaining access to personal information in the normal course of business as well as through hacking.[176] Immediately thereafter, Congress provided an example of such a "thief" who engaged in identity theft *and* identity fraud by accessing customer information through his position at a computer software company.[177] Congress also discussed a fraud ring that had supplied fraudulent Social Security cards, a criminal operation that did not necessarily implicate direct impersonation of another person.[178] In doing so, both

---

[173] *Id.*

[174] *Id.* at 6, *as reprinted in* 2004 U.S.C.C.A.N. 779, 782.

[175] *See, e.g.*, *Berroa*, 856 F.3d at 156 ("The report goes on to provide several examples of identity theft. Notably, each of these examples involved the defendant's use of personal information to pass him or herself off as another person, or the transfer of such information to a third party for use in a similar manner.").

[176] H.R. REP. NO. 108-528, at 4–5, *as reprinted in* 2004 U.S.C.C.A.N. 779, 780–81.

[177] *See id.* at 5, *as reprinted in* 2004 U.S.C.C.A.N. 779, 781.

[178] *See id.*

identity-crime concepts were prevalent in this legislative discussion, with Congress ultimately cautioning that "[t]he insider threat from identity theft *and* identity fraud is a threat to personal security as well as national security."[179]

Second, as noted, the House Report explicitly stated that the eight examples were of identity theft to highlight that minimal prison sentences were "tacit encouragement" for individuals to become repeat offenders.[180] Evidenced above, Congress's use of terminology was inconsistent throughout the House Report. However, this is an instance in which Congress implicitly extended the notion of impersonation to also cover identity fraud. Congress's primary aim in providing the eight examples was to explain how prior law failed to address recidivism by providing inadequate deterrence effects. To further this aim, it had to call attention to real-world scenarios that illustrated sizable gaps between offenses and degrees of punishment.

Notably, instances of disproportionately small punishments for identity crimes are much more likely to fall under impersonation cases. This is because general fraud-facilitation cases more often implicate other areas of the law and trigger additional charges that lead to longer sentences. With this in mind, Congress cherry-picked scenarios to suit its needs, such as the one mentioned above that displayed how William K. Maxfield's violations resulted in a sentence of only ten months. Hence, examples that focused on impersonation were likely more valuable for the overarching demonstrative purpose related to the proportionality of the punishment. Therefore, the use of different terms in the titles likely has little bearing as various statements in the record suggest that Congress attempted to cover both identity theft and fraud under the ITPEA.

2. Mandatory penalty enhancements.

Another consideration in this analysis is the fact that the aggravated identity theft provision is a mandatory penalty enhancement, which has implications for interpreting congressional intent. Recall that under § 1028A(a)(1), a violation of the aggravated identity theft provision mandates a two-year consecutive penalty enhancement; this penalty enhancement is in addition to any term of imprisonment for the underlying offense enumerated

---

179 *Id.* (emphasis added).

180 *Id.*

in the provision.[181] The provision expressly prohibits a judge from ordering the sentence to run concurrently with that of the underlying offense.[182] It also prohibits the court from sentencing a convicted defendant to probation[183] and from reducing the underlying term of imprisonment.[184]

Taken as a whole, the mandatory minimum sentences associated with § 1028A reflect Congress's concern with high-stakes identity theft recidivism as well as its frustration with the inconsistent application of the Federal Sentencing Guidelines.[185] Still, it is valuable to keep in mind the recent proliferation in the application of the aggravated identity theft provision. According to the United States Sentencing Commission, "the percentage of identity theft offenders convicted under section 1028A has steadily increased since shortly after the statute was enacted, more than doubling from 21.9 percent in fiscal year 2006 to 53.4 percent in fiscal year 2016."[186] Furthermore, "[s]ection 1028A aggravated identity theft offenses also increased as a portion of all offenses carrying mandatory minimum penalties. Section 1028A offenses accounted for 7.2 percent of offenses carrying a mandatory minimum penalty in fiscal year 2016, increasing from 4.0 percent in 2010."[187]

Given this uptick and the general severity associated with a mandatory consecutive penalty enhancement, some may argue that a broader reading of the provision would result in its application to situations beyond which Congress had originally contemplated, resulting in a relatively punitive interpretation. That is, less harmful misuse of personal information is potentially more common in today's technological environment, and some may fear that such minor misuses might implicate the statute and result in disproportionate punishments relative to the offenses.

---

[181] 18 U.S.C. § 1028A(a)(1).

[182] 18 U.S.C. § 1028A(b)(2).

[183] 18 U.S.C. § 1028A(b)(1).

[184] 18 U.S.C. § 1028A(b)(3).

[185] *See* H.R. REP. NO. 108-528, at 7, *as reprinted in* 2004 U.S.C.C.A.N. 779, 783 ("At the Subcommittee and full Committee mark-ups Crime Subcommittee Chairman Coble noted, 'opponents of mandatory minimums would have a more compelling case if they could assure the Congress that the judges were faithfully following the Federal Sentencing Guidelines. And I think, sadly, there's evidence that doesn't support that.'").

[186] U.S. SENT'G COMM'N, MANDATORY MINIMUM PENALTIES FOR IDENTITY THEFT OFFENSES IN THE FEDERAL CRIMINAL JUSTICE SYSTEM 14 (2018).

[187] *Id.* at 15.

There are several responses to these concerns. First, the fact that the use of a means of identification must occur "during and in relation to any felony violation enumerated in subsection (c)" limits the concern of overapplication.[188] The predicate felonies limit and anchor the aggravated identity theft provision to situations that have already triggered provisions that proscribe more severe conduct such as embezzlement, bank and medical fraud, and false personation in Social Security contexts. Accordingly, more commonplace misusers of personal identifying information will not be subjected to the possibility of a penalty enhancement. For example, someone's use of another person's picture on a social media profile—while potentially compromising that person's public image and privacy interests—will not necessarily trigger the statute.

Second, when analyzed against the backdrop of the enactment of the ITPEA, the aggravated identity provision aptly serves as a measure to combat the sweeping issues that arose as a result of the Information Age. With this technological evolution came additional avenues for identity crimes, creating opportunities for criminal activity in contexts such as online banking and digital transfers of confidential data. To rid the provision of its broader reach would impermissibly counteract Congress's aim of protecting helpless consumers in an evolving computer-driven society.

This is not to say that the imposition of mandatory minimums alone meant that Congress wanted a broad reading of "uses." Rather, given the aforementioned legislative history regarding contemporaneous changes in technology, Congress likely implemented the mandatory minimums knowing at the outset the wide scope of coverage that its reactive law would take on. Further, people are increasingly expected to offer their personal information online—be it for their jobs, for browsing websites that track data usage, or for signing up for digital subscriptions. Therefore, the mandatory minimum sentences associated with the aggravated identity theft provision not only act as strong deterrents for the actors who caused a total of $56 billion in losses to U.S. consumers in 2020,[189] but also embodies Congress's intent to guide and protect average consumers in a potentially hostile space that increasingly threatens financial harm and dire reputational costs.

---

[188] *See* 18 U.S.C. § 1028A(a)(1).

[189] John Buzzard & Tracy Kitten, *2021 Identity Fraud Study: Shifting Angles*, JAVELIN STRATEGY & RSCH. (Mar. 23, 2021), https://perma.cc/AVF8-A9FR.

C. The Impropriety of the Rule of Lenity

The application of the rule of lenity is improper in the context of the aggravated identity theft provision. Under the judicial doctrine of the rule of lenity, "a court, in construing an ambiguous criminal statute that sets out multiple or inconsistent punishments, should resolve the ambiguity in favor of the more lenient punishment."[190] This doctrine is related to the notion of fair-warning challenges, which states that "no one should be held criminally liable for conduct that he or she could not reasonably understand to be prohibited."[191]

The aggravated identity theft provision—and particularly the role of "uses"—does not rise to a level of grievous ambiguity so as to trigger the rule of lenity. Legal scholars have characterized the doctrine as a "last resort" that is subjugated to other indicators of meaning.[192] Further, "[t]he mere possibility of articulating a narrower construction [ ] does not by itself make the rule of lenity applicable."[193] In this case, a variety of interpretative tools are available and operative. The Fourth Circuit, among others, has provided an analytical backdrop that explains the broad plain meaning of the term[194] consistent with the textual analysis conducted in this Comment. Moreover, an analogous case that has wrangled with similar statutory language arrived at the same conclusion.[195] In addition, the surplusage canon counters the canons of noscitur a sociis and ejusdem generis, granting "uses" a differentiated meaning so as to not encroach upon the definitional territory of the other two verbs in the statute.

The amendment notes to the ITPEA support the outcome of this Comment's textual analysis: the meaning of the aggravated identity theft provision is unambiguous, though broad. Initially,

---

190 *Rule of lenity*, BLACK'S LAW DICTIONARY (11th ed. 2019).

191 *Fair-warning challenge*, BLACK'S LAW DICTIONARY (11th ed. 2019).

192 *See, e.g.*, David S. Rubenstein, *Putting the Immigration Rule of Lenity in Its Proper Place: A Tool of Last Resort After* Chevron, 59 ADMIN. L. REV. 479, 493 (2007) ("Like the criminal rule of lenity, its immigration counterpart is a doctrine of last resort that comes into operation only after other interpretive aids fail to yield sufficient insight into Congress's intent.").

193 *Smith*, 508 U.S. at 239; *see also id.* ("Instead, that venerable rule is reserved for cases where, '[a]fter "seiz[ing] every thing from which aid can be derived,"' the Court is 'left with an ambiguous statute.'" (quoting United States v. Bass, 404 U.S. 336, 347 (1971) (quoting United States v. Fisher, 6 U.S. (2 Cranch) 358, 386 (1805))).

194 *See, e.g.*, *Abdelshafi*, 592 F.3d at 607.

195 *See Smith*, 508 U.S. at 236–37. *But see Bailey*, 516 U.S. at 143.

the title-and-headings canon posed auxiliary issues for the general-misuse camp. Specifically, the differences between the titles of the identity fraud provision and the aggravated identity theft provision could have suggested an underlying conceptual divide between fraud and theft. Given the assertions in the House Report, however, Congress likely used these terms to refer to the use of personal information to perpetuate or facilitate fraud.[196] And although the eight listed examples primarily involve impersonation, they serve a particular illustrative purpose that does not affect the meaning of "uses" and thus carry little weight.

Moreover, as a matter of policy, the enumeration of specific categories of predicate felonies alleviates any concern that a broad reading of "uses" would result in the statute's application to situations beyond what Congress intended. This is because the statute limits the punishment to actions that occur during or in relation to said predicate offenses, which cabins liability to more serious offenders.[197] Taken as a whole, these factors suggest that the term "uses" in § 1028A should take on a broader meaning to encompass the use of means of identification in the general facilitation of fraud, a tenable outcome as a matter of plain meaning, legislative considerations, and policy.

IV. ADVANTAGES OF THE MAJORITY APPROACH IN PRACTICE

This final Part illustrates the advantages of the majority approach in practice. Under the general-misuse interpretation, the term is not ambiguous and the rule of lenity does not apply. As such, the defendant need only generally misuse another's information in the facilitation of fraud. With this approach, courts are better equipped to assess the aggravated identity theft provision in more modern, technological contexts. Accordingly, the following sections examine the benefits of relying on the unambiguous, though broad, meaning of the aggravated identity theft provision, specifically in the contexts of digital political dissent and vigilante hacktivism in online ecosystems.

A. Applications in Digital Political Dissent

The general-misuse approach is beneficial in the contexts of digital political dissent and hacking. As a general primer, hacking

---

196 *See* H.R. REP. NO. 108-528, at 4–5 *as reprinted in* 2004 U.S.C.C.A.N. 779, 780–81.
197 *See* 18 U.S.C. § 1028A(a)(1).

falls into the categories of black-hat, white-hat, or grey-hat hacking.[198] Black-hat hacking, or malicious hacking, involves an illegal attempt to gain access to a computer system.[199] White-hat hacking, or ethical hacking, involves an authorized attempt to gain unauthorized access to a computer system to help assess security vulnerabilities.[200] Grey-hat hacking involves a mix of black hat hacking and white hat hacking.[201] This practice exposes security vulnerabilities without self-serving motivations, but hackers often do so through illegal methods.[202]

In cases that involve fraud schemes that implicate impersonation, both the general-misuse and impersonation approaches cover the proscribed conduct. For example, in *United States v. Hammond*,[203] Hammond engaged in both black-hat and grey-hat hacking. Beginning in 2011, Hammond mounted a cyber assault on Strategic Forecasting, Inc. ("Stratfor"), an information analysis company.[204] In the process, he stole confidential information including "approximately 60,000 credit card numbers and associated data belonging to clients of Stratfor" and "records for approximately 860,000 Stratfor clients, including individual user IDs, usernames, encrypted passwords, and email addresses."[205]

The defendant then publicly disclosed stolen data that arguably shed light on the corruption of Stratfor, including bribery, insider trading, and corrupt connections with large corporations and government agencies.[206] He also "used some of the stolen credit card data to make at least $700,000 worth of unauthorized charges,"[207] including "large donations to charities and nonprofits."[208] In addition to pleading guilty for conspiracy to violate the Computer Fraud and Abuse Act,[209] the defendant was indicted for aggravated identity theft.[210] He was ultimately sentenced to ten

---

198 ALANA MAURUSHAT, ETHICAL HACKING 20 (2019).

199 *See id.* at 20.

200 *See id.*

201 *See id.* at 20–21.

202 *See id.*

203 No. 12 Crim. 185(LAP), 2013 WL 637007 (S.D.N.Y. Feb. 21, 2013).

204 *Id.* at *1–2.

205 *Id.* at *1.

206 MAURUSHAT, *supra* note 198, at 75.

207 *Hammond*, 2013 WL 637007, at *1.

208 Janus Kopfstein, *Hacker with a Cause*, NEW YORKER (Nov. 21, 2013), https://perma.cc/7N4P-3PVX.

209 Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030).

210 *Hammond*, 2013 WL 637007, at *1.

years in federal prison.[211] Given that the credit card fraud implicated impersonation, both the general-misuse and impersonation approaches would support adding the two-year sentencing enhancement in this scenario.

However, consider an alternative situation in which Hammond—now less technologically sophisticated in his individual capacity—did not use the stolen credit card data to make unauthorized charges. Instead, he facilitated a third-party hacking collective's attempt to gain access and to hold Stratfor's client data hostage until Stratfor vowed to change its corrupt behavior for the public good. As a threat, he communicated to Stratfor that if it did not comply, he would tell the third party to release all of Stratfor's clients' data on an online forum. Not only would this cause lethal reputational harm to Stratfor, it would also destroy the financial standing of Stratfor's individual clients; however, Hammond believed that this was a necessary risk and sacrifice to achieve his broader aims. Under this set of facts, Hammond would have used the personal identifying information in furtherance of his general goal of shedding light on Stratfor's corrupt practices.

Here, the impersonation approach would not have reached Hammond's own conduct, given that he was not impersonating any of the owners of the data that he was holding hostage. Moreover, he would not have been directly transferring or possessing the means of identification himself. Therefore, the general-misuse approach would better address this situation by enhancing penalties for Hammond's behavior given the risk of personal loss via the leaked information. This scheme to hold means of identification hostage is the type of action that Congress wanted to proscribe during the technology boom of the early 2000s.[212] The centrality of the personal information to the scheme—evidenced by Hammond's threat to release the data—is an exemplary manifestation of Congress's fear of consumer harm. This concern is particularly apparent in this situation given that a third party, with Hammond's facilitation, misappropriated the personal infor-

---

[211] Kopfstein, *supra* note 208.

[212] In a strict sense, one could construe this isolated action as possession. As a practical matter, however, courts are largely unwillingly to read possession alone as implicating the aggravated identity theft provision, resorting to the more general definitional space captured by "uses." *See generally* Part II. Consequently, a shift to a broader understanding of statutory language becomes necessary in situations that sit squarely within the textual confines and purpose of the statute.

mation of 860,000 individuals—an astonishing figure that highlights the ease and efficiency with which contemporary wrongdoers can improperly access and compromise data. As such, the majority approach aptly accounts for the root of the harms to financial reputation and personal inconveniences that very likely would have occurred in this alternative fact pattern.[213]

B. Predicate Felonies as a Safeguard

The general-misuse approach is particularly valuable in borderline cases that stretch the traditional concept of "use." In such situations, the perpetrator utilizes the means of identification neither to impersonate nor to act on behalf of another. For example, after *Hammond*, Barrett Brown—a journalist and online activist—copied and pasted a public link to the Stratfor Hack documents in an internet chat channel entitled #ProjectPM, "a crowd-sourced think tank that focuses on government intelligence contractors."[214] A fervent spokesperson of hacktivist collective Anonymous, he supported the Stratfor Hack and later uploaded a YouTube video in which he threatened an FBI agent assigned to the matter.[215]

In addition to charging Brown for the various predicate offenses, the government indicted Brown for aggravated identity theft for using the "means of identifying ten individuals in Texas, Florida, and Arizona, in the form of their credit card numbers and the corresponding CVVs for authentication as well as personal addresses and other contact information."[216] In response, some commentators have argued that the application of the aggravated identity theft provision in such cases may have detrimental ef-

---

[213] Conspiratorial data-hostage and ethical-hacking situations like this example are relatively common in contemporary computer ecosystems; modern ransomware capabilities have made this technology a compelling route for pecuniary or political gain by both state and nonstate actors through online civil disobedience, hacktivism, counterhacking, and whistleblowing. *See* MAURUSHAT, *supra* note 198, at 7–9. In her work, Professor Alana Maurushat documented over two hundred high-profile ethical hacking incidents that occurred from 1999 to 2018 carried out by major vigilante groups from around the world. *See* MAURUSHAT, *supra* note 198**,** at 57–95.

[214] Kristin Bergman, *Adding up to 105: The Charges Against Barrett Brown*, DIGIT. MEDIA L. PROJECT (Aug. 6, 2013), https://perma.cc/4S95-PM28.

[215] *See id.*; *see also* Philip F. DiSanto, Note, *Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud*, 115 COLUM. L. REV. 941, 942–43 (2015).

[216] Bergman, *supra* note 214.

fects on free speech for reporters using digital channels of communication.[217] Specifically, some scholarship suggests that courts should heighten the requisite mens rea in these situations by requiring intent that personal information be used for malicious purposes.[218]

Even in borderline cases, however, courts should apply the aggravated identity theft provision in accordance with the broad plain meaning of the text. Given the relative rarity of journalists who commit the predicate felonies enumerated in the statute, there will likely be minimal "dire consequences for press freedom"[219] that would justify a heightened state of mental culpability that others have suggested.[220] The vast majority of reporters do not commit predicate felonies while engaging in their journalistic activities and therefore will likely not meet Brown's fate. This bypasses concerns about free-speech-chilling effects. Thus, as long as an underlying offense is present, courts should continue to apply the aggravated identity theft provision even in cases in which the defendant's use of the personal information is relatively distant from the "actual" fraud. This reading best reflects the statute's main purpose of protecting consumers and companies from financial and reputational losses that would occur regardless of whether the perpetrator intended said losses.

---

[217] *See, e.g.*, DiSanto, *supra* note 215, at 954 ("[C]ommentators and civil rights organizations have referred to the government's interpretation of §§ 1028 and 1028A as troubling for news organizations and journalists that do not fall within traditional definitions."); Hanni Fakhoury & Trevor Timm, *Barrett Brown Prosecution Threatens Right to Link, Could Criminalize Routine Journalism Practices*, ELEC. FRONTIER FOUND. (July 19, 2013), https://perma.cc/4S4K-NA6H ("While one would assume linking to the list is a First Amendment-protected activity—given the journalists had nothing to do with stealing the passwords—Barrett Brown is currently under indictment, in part, for remarkably similar behavior. And if he is convicted, it could have dire consequences for press freedom.").

[218] DiSanto, *supra* note 215, at 979.

[219] Fakhoury & Timm, *supra* note 217.

[220] There are other types of digital journalism, however, that may face more consequences related to press freedom than the instant cases. For example, Julian Assange, the founder of WikiLeaks, was indicted under 18 U.S.C. §§ 371, 973, and 1030 for disclosing national defense information and conspiring to commit computer intrusion. *See In re* Reporters Comm. for Freedom of the Press to Unseal Crim. Prosecution of Assange, 357 F. Supp. 3d 528 (E.D. Va. 2019). If Assange's actions had involved the means of identification of another person and he had been charged under the aggravated identity theft provision, then the situation would have implicated issues concerning the First Amendment, the public and journalistic interests in the unfettered communication of information, classified information, and national security, which are outside the scope of this Comment.

CONCLUSION

To summarize, it is improper to reach the rule of lenity because the aggravated identity theft provision is unambiguous and because there are practical advantages to the general-misuse approach. When enacting the ITADA, Congress sought to develop and expand its legislation regarding identity theft and fraud to adapt to a changing social and technological environment. The legislation's ultimate shortcomings led Congress to bolster identity theft and fraud laws through the ITPEA, addressing concerns over recidivism.

In addition to the outcome of the textual analysis, courts in comparable situations have similarly focused on the broad ordinary meaning of the term "uses." Furthermore, the surplusage canon counters the canons of noscitur a sociis and ejusdem generis, granting "uses" a meaning that prevents it from duplicating the meaning of the other two verbs in the provision. Moreover, the House Report and amendment notes to the ITPEA suggest that the use of the different terms "identity fraud" and "identity theft" in these statutes has little bearing on the meaning of § 1028A. As a matter of policy, the construction of the aggravated identity theft provision itself—with the penalty enhancements anchored in enumerated predicate felonies—quells the concerns that a broad reading of the provision would result in its application to situations beyond which Congress had originally contemplated.

Finally, the practical advantages of the general-misuse approach are especially apparent in a technological context. Under the general-misuse interpretation, where the defendant need only generally misuse another's information in the facilitation of fraud, courts are ultimately better equipped to apply the aggravated identity theft provision in contexts including digital political dissent and hacktivist activities.