PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 19-1404

_____

CHRISTOPHER RAD,
Petitioner

v.

ATTORNEY GENERAL UNITED STATES OF AMERICA

_____

On Petition for Review of a Decision of
the Board of Immigration Appeals
[Agency No. A034-985-319]
Immigration Judge: John P. Ellington

_____

Argued September 15, 2020

Before: KRAUSE, RESTREPO, and BIBAS, *Circuit Judges*

(Opinion Filed: December 21, 2020)

Christopher Rad
Pike County Correctional Facility
175 Pike County Boulevard
Lords Valley, PA 18428
Pro Se Petitioner

Jacob A. Bashyrov
Craig A. Newell, Jr.**[Argued]**
United States Department of Justice
Office of Immigration Litigation
P.O. Box 878
Ben Franklin Station
Washington, DC 20044
Counsel for Respondent

Ana Builes
Hannah Mullen **[Argued]**
Tyler Purinton
Adam Walker
Brian S. Wolfman, Esq.
Georgetown University Law Center
600 New Jersey Avenue, N.W., Suite 312
Washington, DC 20001

Bradley Girard
Americans United for Separation of Church and State
1310 L Street, N.W., Suite 200
Washington, DC 20005
Court-Appointed Amicus Curiae

OPINION OF THE COURT

KRAUSE, *Circuit Judge.*

Since its earliest days, the internet has provided a forum for users to share ideas, do business, and gather information in relative anonymity. Whether the CAN-SPAM Act's rarely-invoked but potentially far-reaching criminal provisions alter that paradigm is the central question presented by this appeal. *See* 18 U.S.C. § 1037(a). In one view, the Act implements a sweeping anti-anonymity principle that compels individuals and businesses to disclose their identity in every commercial email they send and every domain name they register. Recognizing the troubling constitutional and practical consequences of this approach, we read the Act differently. Rather than penalizing everyday practices, the Act reflects and reinforces longstanding norms. So long as marketers refrain from making false statements in contexts where consumers have come to expect accuracy, their conduct comports with the norms embedded in the architecture of the internet—and with the Act. With this narrow, norms-based interpretation in mind, we conclude that Petitioner's convictions for conspiring to violate the CAN-SPAM Act necessarily entail deceit, and therefore satisfy the first element of an aggravated felony under 8 U.S.C. § 1101(a)(43)(M)(i).

The second element, that Petitioner's crimes inflicted victim losses over $10,000, is a different story. In reviewing a removal order, we are bound by one of administrative law's most fundamental principles: We judge the agency's decision "solely by the grounds [it] invoked," *SEC v. Chenery Corp.*, 332 U.S. 194, 196 (1947). The Board of Immigration Appeals' initial removal order overlooked crucial differences between sentencing hearings and immigration proceedings, so we remanded. But the revised order rests on the same flawed understanding of the loss element as its predecessor, and we therefore cannot approve the agency's analysis. Even as we reject the Board's rationale, however, we hold that intended losses, not just actual ones, may meet the loss requirement for Petitioner's conspiracy offenses, see 8 U.S.C. § 1101(a)(43)(U). Because the Board never addressed this possibility, we are compelled to provide yet another opportunity for it to examine the loss element.

I. Factual and Procedural Background

A. The CAN-SPAM Act

To provide context for this appeal, we offer a brief introduction to the CAN-SPAM Act. The Act's purpose is to address the harms caused by "unsolicited commercial . . . [e]mail," otherwise known as spam. 15 U.S.C. § 7701(a)(2). To that end, the Act empowers consumers to sue marketers who relay misleading messages or refuse to honor opt-out requests. *Id*. § 7703 *et seq*. It also enables prosecutors to bring criminal charges against spammers who embrace especially

abusive tactics. *See* 18 U.S.C. § 1037(a). Two of those tactics are the subject of this appeal.

The first involves falsifying an email's header information. By definition, a header records a message's "source, destination, and routing." 15 U.S.C. § 7702(8). In most cases, a sender's computer populates the header with accurate information about the message's origin. *See* Dan Boneh, *The Difficulties of Tracing Spam Email* 2-3, FTC (Sept. 9, 2004), https://perma.cc/7NG3-M4MV. In some cases, however, spammers manipulate headers to report false information. *Id*. This tactic, called "spoofing," confuses spam filters, misleads recipients, and impedes investigators. *Id*. at 4, 11. The Act therefore prohibits it. *See* 18 U.S.C. § 1037(a)(3).

The second tactic consists of registering a domain name using a false identity. As a general matter, a domain name describes an "alphanumeric designation which is registered with . . . [a] registration authority as part of an electronic address on the [i]nternet." 15 U.S.C. § 7702(4). To prevent multiple users from claiming the same domain, the Internet Corporation for Assigned Names and Numbers (ICANN) administers a registration system. *What ICANN Does and Doesn't Do*, ICANN (June 22, 2012), https://www.icann.org/en/system/files/files/what-icann-does-22jun12-en.pdf. Under ICANN's rules, a registrant cannot reserve a domain without publicly disclosing their contact information. *FAQ: Domain Name Registrant Contact Information*, ICANN (Feb. 25, 2012), https://www.icann.org/resources/pages/faqs-f0-2012-02-25-

en. This requirement makes it easier for law enforcement agencies to investigate fraud, hacking, and other criminal activities conducted over the internet. *See* Jon Leibowitz, *Prepared Statement of the Federal Trade Commission Before ICANN* 4 (June 2006), https://perma.cc/98UG-9L9N. Not surprisingly, spammers sometimes flout ICANN's rules—and avoid the scrutiny those rules facilitate—by registering domain names using false contact information. This tactic, too, violates the Act. *See* 18 U.S.C. § 1037(a)(4).

B. Rad's Trial and Sentencing

Though the CAN-SPAM Act came into force almost two decades ago, its criminal provisions have given rise to only a handful of prosecutions, one of which underlies this case. In 2012, a grand jury approved a nine-count superseding indictment against Petitioner Christopher Rad. According to the indictment, Rad and several co-conspirators acquired shares of penny stocks, "pumped" the prices of those stocks by bombarding investors with misleading spam emails, and then "dumped" their shares on the market at a profit. A.R. 75–76. Of relevance here, Count I charged Rad with conspiring to commit false header spamming, see § 1037(a)(3), false domain name spamming, see § 1037(a)(4), and securities fraud, see 15 U.S.C. §§ 78j and 78ff.[1] At trial, a jury convicted Rad of the

[1] The remaining counts, which charge both substantive and inchoate violations of the CAN-SPAM Act, played no part in the Board's removal decision, and are therefore irrelevant to this appeal.

first two conspiracies, but failed to reach a verdict as to the third.

In preparation for sentencing, the Probation Office circulated a Presentence Investigation Report ("PSR") recommending that the District Court raise Rad's offense level to reflect the losses his crimes inflicted on investors. *See* U.S.S.G. § 2B1.1(b)(1). The PSR began by estimating that Rad realized about $2.9 million in "illicit gains" over the course of the conspiracy. A.R. 42. It then acknowledged that, because "countless victims" purchased stocks "based on the spamming scheme," the losses stemming from Rad's conduct could not "reasonabl[y] be determined." *Id*. at 46. It nonetheless advised the Court to treat Rad's gains as a proxy for victim losses and to lengthen his sentence accordingly. *Id*.; *see* U.S.S.G. § 2B1.1, cmt. n.3(B) ("The court shall use the gain that resulted from the offense as an alternative measure of loss . . . if there is a loss but it reasonably cannot be determined."). For his part, Rad questioned whether his crimes caused any losses and emphasized the absence of evidence "that any single person lost anything" as a result of the conspiracy. A.R. 67.

At sentencing, the District Court ordered Rad to serve a total of seventy-one months in prison, including thirty-five months attributable to Count I. Because neither party introduced a transcript of the sentencing hearing, the administrative record is silent as to how the Court analyzed and

resolved the victim loss issue.[2] We upheld the District Court's judgment on appeal.

C. Removal Proceedings

Not long after the District Court sentenced Rad, the Department of Homeland Security ("DHS") initiated removal proceedings. Under the Immigration and Naturalization Act ("INA"), DHS retains authority to remove noncitizens who commit "aggravated felonies." 8 U.S.C. § 1227(a)(2)(A)(iii). That category includes any crime that (1) "involves fraud or deceit" (2) "in which the loss to the victim or victims exceeds $10,000." *Id.* § 1101(a)(43)(M)(i).

In proceedings before an Immigration Judge ("IJ"), DHS characterized Rad's CAN-SPAM Act convictions as felonies involving deceit and the requisite level of victim losses. The IJ agreed and the Board affirmed.

---

[2] Despite the possible relevance of the transcript of Rad's sentencing hearing, we cannot take judicial notice of materials outside the administrative record. *See Berishaj v. Ashcroft*, 378 F.3d 314, 330 (3d Cir. 2004) ("[C]ourts reviewing the determination of an administrative agency must approve or reject the agency's action purely on the basis of . . . the record compiled before[] the agency itself."); *cf. Nbaye v. Att'y Gen.*, 665 F.3d 57, 59–60 (3d Cir. 2011) (remanding to permit the Board to consider extra-record information in the first instance).

When Rad filed his first petition for review before this Court, DHS urged us to remand to permit the Board to "further consider[]" whether Rad's offenses constitute aggravated felonies. A.R. 318. In explaining why remand was warranted, DHS collected controlling precedents that the Board had failed to address in its initial order. We therefore sent the case back to the Board.

On remand, the agency proceeded to retread the ground it covered in its initial analysis of the loss element. Rather than reviewing evidence from Rad's sentencing hearing, the Board depended on an inference drawn from the criminal judgment. Because "a 35-month sentence was ultimately imposed for [Count I]," the agency reasoned, "the sentencing judge [must have] added *at least* 6 levels based on victim loss—a determination that would have required the court to assess the loss at greater than $40,000." A.R. 5; *see* U.S.S.G. § 2B1.1(b)(1)(D). So, while the Board conceded that "the precise quantum of victim loss is not readily ascertainable," it nevertheless presumed "the amount of loss . . . exceeded $10,000." A.R. 5. Having classified Rad's crimes as aggravated felonies, the agency ordered him removed from the United States.

We now consider Rad's second, timely-filed petition for review.[3]

II. Jurisdiction and Standard of Review

The Board exercised jurisdiction under 8 C.F.R. § 1003.1(b)(3). We retain jurisdiction to consider "whether [Rad]'s conviction qualifies as an aggravated felony because it is a 'purely legal question, and one that governs our own jurisdiction.'" *Fan Wang v. Att'y Gen.*, 898 F.3d 341, 343 (3d Cir. 2018). Our review of that question is plenary. *See Singh v. Att'y Gen.*, 677 F.3d 503, 508 (3d Cir. 2012).

III. Analysis

To demonstrate that Rad's crimes count as aggravated felonies, DHS bears the burden of establishing two elements. *See Kiareldeen v. Ashcroft*, 273 F.3d 542, 553–54 (3d Cir. 2001). The first is that violations of 18 U.S.C. §§ 1037(a)(3) and (a)(4) categorically involve "fraud or deceit." 8 U.S.C. § 1101(43)(M)(i). In analyzing this requirement, "we focus on the crime's statutory elements 'rather than . . . the specific facts

[3] Because Rad brought this appeal pro se, we asked Georgetown University Law Center's Appellate Courts Immersion Clinic to serve as amicus. We express our gratitude to the Clinic for accepting this matter pro bono, and we commend the Clinic for its superb briefing and argument in this complex case. Lawyers who act pro bono fulfill the highest service that members of the bar can offer to indigent parties and to the legal profession.

underlying the crime.'" *Singh*, 677 F.3d at 508 (alteration in original) (quoting *Kawashima v. Holder*, 565 U.S. 478, 483 (2012)). The second element, whether Rad caused over $10,000 in losses, 8 U.S.C. § 1101(43)(M)(i), is a different story. That requirement hinges on "the specific way in which [Rad] committed the crime[s]," and we therefore review the indictment, judgment, presentence investigation report, and any other "sentencing-related material" that sheds light on Rad's conduct. *Nijhawan v. Holder*, 557 U.S. 29, 34, 42 (2009). As we shall see, DHS has met its burden as to the first element, but we must remand for the Board to revisit the second.

A. The Fraud or Deceit Element

The central question presented here is whether 18 U.S.C. §§ 1037(a)(3) and (a)(4) categorically "involve[] fraud or deceit."[4] 8 U.S.C. § 1101(43)(M)(i). In answering this question, we begin by defining deceit; we proceed to survey the scope of the CAN-SPAM Act; and we conclude by asking whether the least-culpable conduct covered by the Act entails deceit. Because the parties focus on deceit, we do the same.

[4] Although prosecutors charged Rad with conspiracy to commit securities fraud, the jury failed to reach a verdict as to that charge. DHS therefore concedes that the conspiracy to commit securities fraud charge does not justify Rad's removal.

1. How the INA Defines Deceit

Our initial task is to stake out the boundaries of the INA's deceit provision. On this front, at least, we need not write on a blank slate. We long ago recognized that the INA uses "deceit" in its commonly accepted legal sense—namely, "the act of intentionally giving a false impression." *Valansi v. Ashcroft*, 278 F.3d 203, 209 (3d Cir. 2002) (citing Black's Law Dictionary 413 (7th ed. 1999)). In the intervening years, at least one of our sister circuits has endorsed this definition; none have disputed it; and the IJ and DHS invoked it in this case. *See James v. Gonzales*, 464 F.3d 505, 508 & n.14 (5th Cir. 2006); *Patel v. Mukasey*, 526 F.3d 800, 802–03 (5th Cir. 2008).

A similar understanding of deceit emerges from one of the Supreme Court's removal cases, *Kawashima v. Holder*, 565 U.S. 478 (2012). There, the Court equated "deceit" with "'the act or practice of deceiving (as by falsification, concealment, or cheating).'" *Id*. at 484 (quoting Webster's Third New International Dictionary 584 (1993)). At its core, this definition turns on the gerund "deceiving," a word that means "caus[ing] to believe the false." *Deceive*, Merriam-Webster Unabridged, https://www.unabridged.merriam-webster.com/unabridged/deceiving (last visited Oct. 15, 2020). That leaves little, if any, practical difference between *Valansi*'s and *Kawashima*'s definitions. Here, for example, §§ 1037(a)(3) and (a)(4) necessarily entail deceit, no matter which formulation applies. To see why, we must abandon the familiar domain of the INA and venture into the *terra incognita* of the CAN-SPAM Act.

2. What the CAN-SPAM Act Prohibits

The categorical approach presupposes that we understand the least-culpable conduct covered by a criminal statute. Yet no controlling cases analyze §§ 1037(a)(3) and (a)(4), and few courts at any level have done so. For their part, the parties paint drastically different pictures of the Act. While DHS depicts the false-header and domain-name spamming provisions as proscribing a specific set of abuses, Amicus portrays those provisions as announcing that all senders of commercial email must comply with a sweeping anti-anonymity principle. We conclude, however, that far from upending pre-existing norms, the Act reflects and reinforces them. To show how it does so, we look first to the Act's text. We then explain why the doctrine of constitutional avoidance supports our narrow reading of the Act. And finally, we identify where Amicus's more expansive construction goes astray.

a) Statutory text

Our inquiry begins—and, as it turns out, largely ends—with the terms of the Act itself. In relevant part, 18 U.S.C. § 1037(a) specifies that:

> Whoever, in or affecting interstate or foreign commerce, knowingly
>
> . . .

> (3) *materially falsifies* header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages, [or]
>
> (4) registers, using information that *materially falsifies* the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts . . .
>
> or conspires to do so, shall be punished . . . .

(emphasis added).

In advancing a far-reaching interpretation of the Act, Amicus downplays these provisions, and instead highlights Congress's subsequent definition of the word "materially":

> For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is *altered or concealed in a manner that would impair the ability of a recipient* of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency *to identify, locate, or respond* to a person who initiated the

> electronic mail message or to investigate the alleged violation.

Id. § 1037(d)(2) (emphasis added). As Amicus would have it, this language transforms a statute designed to target specific abuses into one that compels marketers to divulge their "identi[ty]" and "locat[ion]" in every email they send and every domain name they register. *Id*. For example, Amicus posits that a small business that uses a private ("Anonymous@Generic.com"), vague ("Jane@Sportsfan.com") or whimsical ("Bigfoot@Podiatry.com") email address has "concealed" its "identi[ty]" in a way that risks prosecution. *Id*. And, likewise, Amicus predicts that the thousands of individuals who pay proxies to register domain names on their behalf have similarly "impair[ed]" recipients' ability to "identify" or "locate" them. *Id*. All of this commonplace conduct falls within the scope of §§ 1037(a)(3) and (a)(4), Amicus warns, whenever the sender conveys a sufficient quantity of commercial emails.[5]

[5] The Act applies to defendants who send "multiple" emails, which it defines as "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period." 18 U.S.C. § 1037(d)(3). This element does little to shield everyday conduct from prosecution, given that businesses—from stores announcing a new location to local politicians soliciting donations—often have occasion to send more than a hundred emails in a day.

But we normally refuse to construe statutes as "criminaliz[ing] a broad range of day-to-day activity," and the CAN-SPAM Act is no exception. *United States v. Kozminski*, 487 U.S. 931, 949 (1988). Rather than penalizing everyday practices, the Act implements pre-existing norms. *Cf.* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016) (contending that computer trespass statutes should be interpreted in light of prevailing norms). Since the internet's earliest days, the protocol that permits computers to exchange emails has mandated that a message's header include a field that reflects its sender's address. *See* David Dickinson, Note, *An Architecture for Spam Regulation*, 57 FED. COMM. L.J. 129, 132 (2004). And, for almost as long, ICANN has required registrants to divulge their own contact information, or that of a proxy, when claiming a domain name. *FAQ: Domain Name Registrant Contact Information*, ICANN (Feb. 25, 2012), https://www.icann.org/resources/pages/faqs-f0-2012-02-25-en.

These accountability mechanisms do not dictate that senders reveal who they are or where they are located in every message, and neither does the Act. Instead, senders need only provide recipients with a reliable way of contacting them, whether by replying to a particular account or by communicating through a proxy. So long as individuals and businesses refrain from inserting false contact information in contexts where internet users have come to expect accuracy, their conduct comports with prevailing norms—and with the Act.

Start with the prohibition on false header spamming. What makes Amicus's construction of § 1037(a)(3) so sweeping is that it requires an email address's semantic content to match the sender's reality. If a commercial message arrives from "Jane@sportsfan.com," for example, then Amicus reads the Act as mandating that the sender be named Jane and enjoy sports. In practice, of course, internet users routinely create email addresses that imperfectly or inaccurately reflect their true identities. By the same token, businesses often have occasion to promote their services with addresses that pay homage to fictional mascots ("Bulldog@Almamater.edu"), celebrity endorsers ("Famous_Athlete@Nike.com"), or long-gone founders ("Benjamin_Franklin@Printingpress.com").

Nothing in § 1037(a)(3) criminalizes these commonplace practices. By its terms, that subsection prescribes penalties only for individuals who "falsify," 18 U.S.C. § 1037(a)(3), the "source, destination, and routing information attached to an electronic mail message," 15 U.S.C. § 7702(8). In other words, the information displayed in an email's header must match the address from which the message was actually sent—but not necessarily the sender's true identity. When a business owner conveys communications from "Jane@Sportsfan.com," for example, her emails' headers will report that address, foreclosing the application of § 1037(a)(3) no matter what her name is or whether she follows sports. When a spammer manipulates her messages' headers so that they seem to originate from an account that does not exist or that she does not control, by contrast, she violates the Act. In this way, § 1037(a)(3) promotes the CAN-SPAM Act's

stated purpose of enabling consumers "to decline to receive additional commercial electronic mail from the same source," 15 U.S.C. § 7701(b)(3), without mandating that marketers disclose their identity and location in every message.

The same is true of the prohibition on domain-name spamming. Under Amicus's wide-ranging interpretation of § 1037(a)(4), anyone who employs a proxy service to register a domain name risks federal prosecution. But while using a proxy may sound complex or even criminal, it involves two simple, innocuous steps. First, an individual pays a private registration firm to claim a domain name on his behalf. *See Information for Privacy and Proxy Service Providers*, ICANN (Aug. 31, 2017), available at: https://www.icann.org/resources/pages/pp-services-2017-08-31-en. Second, the firm registers that domain with ICANN, entering its own contact information, rather than that of the individual who will use the domain. *See id*. If the Act outlawed this popular practice, many thousands of individuals might face criminal penalties.

Although the Ninth Circuit has hypothesized that proxy registration "for the purpose of concealing the actual registrant's identity would constitute 'material falsification,'" we respectfully disagree. *United States v. Kilbride*, 584 F.3d 1240, 1259 (9th Cir. 2009). True, many domain-name owners undoubtedly embrace proxy registration because it protects their privacy. But the Act makes it illegal to "falsif[y] the identity of the actual *registrant*," § 1037(a)(4) (emphasis added), and nowhere suggests that the registrant must serve as

the day-to-day owner of a domain. And, given that ICANN's rules expressly permit proxies to enter their own contact information when claiming a domain name on someone else's behalf, we struggle to see how proxy registration reflects "material falsifi[cation]." § 1037(a)(4); *see also Dressler v. Busch Entm't Corp.*, 143 F.3d 778, 781 (3d Cir. 1998) (defining "falsify" as "to engage in misrepresentation or distortion").

Instead, § 1037(a)(4) zeroes in on "registrant[s]"—whether day-to-day domain users or their proxies—who claim a domain using contact information that is not their own.[6] This prohibition reflects ICANN's longstanding rules, which mandate that a registrant disclose its contact information when signing up for a domain name. *FAQ: Domain Name Registrant Contact Information*, ICANN (Feb. 25, 2012), https://www.icann.org/resources/pages/faqs-f0-2012-02-25-en. Like its sister provision, § 1037(a)(4) therefore ensures that recipients retain some way to communicate with the senders of commercial emails, either by replying directly or by contacting a proxy, without compelling senders to share who they are and where they are from with everyone they contact.

[6] Although courts and commentators typically describe § 1037(a)(4) as the domain-name spamming provision, that provision also makes it illegal to register email addresses using false information. Neither the parties nor Amicus identify any reason to treat registration of domain names and email addresses differently.

b) Constitutional avoidance

A contrary construction of §§ 1037(a)(3) and (a)(4) would raise serious constitutional concerns. Though "the overbreadth doctrine does not apply to commercial speech," *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 497 (1982), restrictions on an author's ability to "remain anonymous" nonetheless implicate "the freedom of speech protected by the First Amendment," *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). In the context of political speech, for example, the Supreme Court has long recognized that anonymity advances the First Amendment's core values: It enables "[p]ersecuted groups . . . to criticize oppressive practices," empowers "writer[s] who may be personally unpopular to ensure that readers will not prejudge [their] message[s]," and encourages dissidents to voice their "conscience without fear of retaliation." *McIntyre*, 514 U.S. at 342–43 (first alteration in original) (quoting *Talley v. California*, 362 U.S. 60, 64–65 (1960)).

Whether and to what extent the First Amendment shields speakers who share commercial messages anonymously remains unsettled, but we see no need to wade into that quagmire today. *Cf. Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567 (2011) (recognizing that "a great deal of vital expression" results "from an economic motive"). Understanding the Act narrowly, as limited to false assertions in contexts where recipients expect accuracy, dispels the constitutional concerns that would otherwise accompany Amicus's approach. *See 44 Liquormart, Inc. v. Rhode Island*,

517 U.S. 484, 496 (1996) (observing that the First Amendment protects "the dissemination of *truthful and nonmisleading* commercial messages" (emphasis added)).

c) Amicus's arguments

Notwithstanding its excellent advocacy, Amicus offers an interpretation of the interaction between the Act's substantive provisions, §§ 1037(a)(3) and (a)(4), and its definitions, *id*. § 1037(d), with which we ultimately cannot agree. Boiled down to their essence, (a)(3) and (a)(4) prohibit commercial emailers from "materially falsif[ying]" header or domain name information. *Id*. But Amicus urges that the definition elaborated at § 1037(d)(2) does not just explain what the word "materially" means; instead, it replaces the "materially falsified" term altogether. Should that reading prevail, §§ 1037(a)(3) and (a)(4) would make it a crime to share commercial emails with header or registration information that "conceal" the "identi[ty]" or "locat[ion]" of the sender. *Id*. § 1037(d)(2). That would cast a pall over proxy registration, anonymous emails, and the other commonplace conduct discussed above.

We conclude that this capacious interpretation is incompatible with the Act's text and structure. Most important, understanding § 1037(d)(2) as modifying the "materially falsifies" term would render the verb "falsifies" superfluous, a disfavored and here unnecessary outcome. *See Corley v. United States*, 556 U.S. 303, 314 (2009). It would be equally difficult to square with § 1037(d)'s structure. That

subsection defines specific terms, set off in a distinct typeface, including "loss," (d)(1), "multiple," (d)(3), and "materially," (d)(2). By so designating the term "materially," and not the term "materially falsifies," Congress sent a strong signal that (d)(2)'s definition modifies that word alone.

Should any doubt remain, a comparison between § 1037(d)(2) and its civil counterpart confirms our conclusion. In 15 U.S.C. § 7704(a)(1), Congress authorized civil suits against senders who dispatch "materially false" or "materially misleading" emails. The drafters went on to articulate a series of definitions, including the following:

> [T]he term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

Id. § 7704(a)(6). If this language seems familiar, that is because it tracks § 1037(d)(2) almost word for word. Indeed, the only meaningful difference is that § 7704(a)(6) leaves no

doubt that it modifies the word "materially," not the term "materially false." We see little reason to distinguish § 1037(d)(2) and § 7704(a)(6), and good reason to read them in parallel, given that Congress is unlikely to have intended to enact a criminal provision that sweeps more broadly than its civil analogue. *See United States v. McKie*, 112 F.3d 626, 632 (3d Cir. 1997) (recognizing that our normal practice is to "interpret criminal statutes strictly").

The bottom line is that we decline Amicus's invitation to construe §§ 1037(a)(3) and (a)(4) as requiring that commercial emailers adhere to an anti-anonymity principle. Instead, we embrace a narrow, norms-based reading that reflects the Act's text. Having traced the boundaries of the Act's criminal provisions, and having found this unfamiliar territory to be smaller and less dangerous than it may first appear, we are now equipped to answer the categorical question at the heart of this appeal.

3. Why §§ 1037(a)(3) and (a)(4) Involve Deceit

With a definition of deceit in mind, and a map of the CAN-SPAM Act in view, all that remains is to decide whether the prohibitions on false header and domain name spamming "necessarily entail" deceit.[7] *Kawashima*, 565 U.S. at 484. In

[7] That Rad was convicted of conspiring to violate §§ 1037(a)(3) and (a)(4), rather than substantive violations of those provisions, does not alter our analysis of this element. Because "[c]onspiracy to commit an aggravated felony is itself

applying the categorical approach, we "presume that [Rad's] conviction 'rested upon [nothing] more than the least of th[e] acts' criminalized, and then determine whether even those acts are encompassed by the generic federal offense." *Moncrieffe v. Holder*, 569 U.S. 184, 190–91 (2013) (quoting *Johnson v. United States*, 559 U.S. 133, 137 (2010)) (second and third alteration in original). As it happens, our adoption of a norms-based reading of the Act requires that we resolve this issue in DHS's favor.

To see why, a brief review of the Supreme Court's decision in *Kawashima* is essential. That case centered on 26 U.S.C. § 7206(1), a provision that makes it illegal to insert false statements in a tax return. To prove a violation of § 7206(1), the government must establish "that the document in question was false as to a material matter, that the defendant did not believe the document to be true and correct as to every material matter, and that he acted willfully with the specific intent to violate the law." *Kawashima*, 565 U.S. at 483. Because a defendant cannot be convicted without "knowingly and willfully submitt[ing] a tax return that [i]s false as to a material matter," the Court held that § 7206(1) embodies deceit. *Id*. at 484.

---

an aggravated felony," we "proceed as though [the non-citizen] had been convicted of the substantive offense . . . though in fact he [was convicted of] conspiracy to commit that offense." *Tran v. Gonzales*, 414 F.3d 464, 468 n.3 (3d Cir. 2005) (citing 8 U.S.C. § 1101(a)(43)(U)).

The same logic extends to §§ 1037(a)(3) and (a)(4). In *Kawashima*, the relevant offense concerned the entry of false information in a tax return, a document that ordinarily contains truthful statements. Here, likewise, the Act targets senders who falsify email headers and domain name registration entries, both contexts where consumers expect accuracy. When it comes to § 1037(a)(3), for example, recipients presume that header information reflects a sender's email address. Any deviation from that norm risks giving readers "a false impression" as to a message's origin. *Valansi*, 278 F.3d at 209 (internal quotation marks omitted); *see also Kawashima*, 565 U.S. at 484 (classifying "falsification" as a form of "deceit"). And when it comes to § 1037(a)(4), ICANN's longstanding rules mandate accurate disclosure of a registrant's contact information. In that context, too, falsification tends to cause recipients, investigators, and internet service providers "to believe what is false." *Valansi*, 278 F.3d at 211. We therefore conclude that, like the provision at issue in *Kawashima*, §§ 1037(a)(3) and (a)(4) necessarily entail deceit.

Neither of Amicus's counterarguments convinces us otherwise. Its main contention is that many types of conduct contravene the CAN-SPAM Act without implicating deceit. What unites Amicus's examples is that they assume that any mismatch between a commercial emailer's address and his true identity triggers liability under § 1037(a)(3). But, as we explained already, no matter whether a message comes from a

private, vague, or whimsical address, the sender remains safe from prosecution unless he manipulates the email's header.[8]

This point is best illustrated by *Kilbride*, a CAN-SPAM Act prosecution that Amicus argues did not feature fraud or deceit. The *Kilbride* defendants altered their emails' headers by "tak[ing] the user name of the person receiving the email and put[ting] it in the user name space of the return path." *United States v. Kilbride*, 507 F. Supp. 2d 1051, 1062 (D. Ariz. 2007). For example, if the defendants sent an email "using the domain name 'shouldertricks.com' and [if] the email was

[8] A related issue—albeit one that neither the parties nor Amicus explore—is whether providing ICANN with contact information that many observers will recognize as false qualifies as deceit. In theory, for instance, a domain registrant could list her mailing address as Mars, Atlantis, or El Dorado. These examples may well involve material falsification within the meaning of the CAN-SPAM Act, given that the use of a false address makes it more difficult for investigators to locate the sender. *See* 18 U.S.C. § 1037(d)(2). But even these hypotheticals entail deceit. While listing one's home address as Mars may come across as obviously untrue to an average adult, it will still "giv[e] a false impression" to children and the credulous. *Valansi*, 278 F.3d at 209. And *Kawashima* implicitly rejected a parallel hypothetical: A conceivable way of falsifying a tax return would be to include an imaginary number or a figure with an impossible number of digits; yet this possibility failed to prevent the Supreme Court from classifying § 7206(1) as a crime that categorically entails deceit. *See Kawashima*, 565 U.S. at 483–84. We follow the same approach here.

received by an individual with the email address of 'trresa@aol.com,' [the] program would . . . show a return path for the email of 'trresa@shouldertricks.com.'" *Id.* Amicus makes much of *Kilbride* because, as DHS admits, "[n]o reasonable recipient would have been misled into thinking he sent himself [emails]." Dep't's Supp. Br. at 25. But recipients (or, as is more likely, law enforcement investigators) may well have been misled into thinking the messages originated from the account displayed in the headers. That constitutes deceit.

Amicus's fallback argument draws on the CAN-SPAM Act's larger structure. In the subsection immediately preceding §§ 1037(a)(3) and (a)(4), Congress made it a crime "to relay or retransmit" commercial emails "with the intent to deceive or mislead recipients . . . as to the origin of such messages." 18 U.S.C. § 1037(a)(2). According to Amicus, the drafters' use of the verb "deceive" in an adjacent provision establishes that the "materially falsifies" element cannot be coextensive with deceit. *See Russello v. United States*, 464 U.S. 16, 23 (1983). We agree that the juxtaposition of §§ 1037(a)(3) and (a)(4), on one hand, and (a)(2), on the other, reveals that "falsifi[cation]" and "decei[t]" are not identical. That provides little help to Rad, however, because the Act reflects that §§ 1037(a)(3) and (a)(4) focus more narrowly than (a)(2), not more broadly. Unlike their sister provision, the prohibitions on header and domain name spamming include the limiting adverb "materially." §§ 1037(a)(3), (a)(4). They also hinge on "falsification," *id.*, and therefore exclude other ways of deceiving others, such as "concealment or cheating," *Kawashima*, 565 U.S. at 484. So, while the Act's structure

suggests that §§ 1037(a)(3) and (a)(4) may not criminalize *all* deceitful conduct, it confirms that the *only* conduct those provisions prohibit involves deceit.

In the end, our narrow, norms-based reading of §§ 1037(a)(3) and (a)(4) turns out to be decisive.[9] Because the Act targets false statements made in contexts where internet users expect accuracy, even the least culpable violations entail deceit. We thus affirm the Board's judgment that Rad's offenses fulfill 8 U.S.C. § 1101(a)(43)(M)(i)'s fraud or deceit requirement. That does not end our inquiry, however, because DHS also bears the burden of showing that Rad's crimes reflect over $10,000 in victim losses. To that subject, we now turn.

[9] We acknowledge that our reading diverges from the Board's. But the Board's interpretation, which construes the Act's interstate commerce element as including a mens rea requirement, conflicts with well-settled interpretative principles. *See Torres v. Lynch*, 136 S. Ct. 1619, 1631 (2016) ("[C]ourts have routinely held that a criminal defendant need not know of a federal crime's interstate commerce connection to be found guilty."). And, "[a]lthough we give *Chevron* deference to the [Board]'s interpretation of the aggravated felony provisions of the INA if we determine that the statute is ambiguous," the Board "is not entitled to *Chevron* deference as to whether a particular federal criminal offense is an aggravated felony." *Bobb v. Att'y Gen.*, 458 F.3d 213, 217 n.4 (3d Cir. 2006).

B. The Victim Loss Element

The final question we confront is whether Rad's crimes inflicted victim losses that exceed the statutory threshold. Unlike the categorical approach applied above, our evaluation of this element depends on "the specific way in which an offender committed the crime" and we therefore retain authority to consider any "sentencing-related material[]" that sheds light on Rad's conduct. *Fan Wang*, 898 F.3d at 349–50 (quoting *Nijhawan*, 557 U.S. at 42). In reviewing the Board's analysis of that material, we are bound by one of administrative law's most fundamental principles: We must judge an agency's decision "solely [on] the grounds [it] invoked." *Dia v. Ashcroft*, 353 F.3d 228, 241 (3d Cir. 2003) (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 196 (1947)).[10] Because the challenged order overlooks crucial differences between sentencing hearings and immigration proceedings, we cannot adopt the Board's reasoning. Below, we catalog the problems with its analysis, and then explain our decision to give DHS one last chance to make its case.

1. Where the Challenged Order Errs

To understand why remand is required, one need look no further than the Board's order. Rather than examining evidence from Rad's sentencing hearing, the agency fixated on

[10] "Where, as here, the B[oard] issues a written decision on the merits, we review its decision, not that of the IJ." *Moreno v. Att'y Gen.*, 887 F.3d 160, 163 (3d Cir. 2018) (internal quotation marks omitted).

the outcome of that proceeding. Working backwards from the thirty-five month sentence the District Court imposed for Count I, the Board surmised that the Court must have "added *at least* 6 levels based on victim loss—a determination that would have required the court to assess the loss at greater than $40,000." A.R. 5. Otherwise, the Board reasoned, it would have been "mathematically impossible" for the Court to sentence Rad to as many months in prison as it did. *Id*. Having inferred that the District Court found Rad responsible for over $10,000 in losses under the Sentencing Guidelines, the Board presumed it could do the same under the INA. What underlies this result is the premise that loss determinations follow the same rules no matter whether they occur in the course of an immigration proceeding or a sentencing hearing.

But that premise is fundamentally flawed. Rather than codifying similar standards for calculating losses, the Guidelines and INA prescribe frameworks that differ in almost every respect: They require that losses be connected to different types of conduct, elaborate different tests for deciding when an offender's gains serve as a proxy for victims' losses, and hold the government to different burdens of proof. *See Singh*, 677 F.3d at 511 (describing the Guidelines and INA as "apples and oranges"). We outline these distinctions below, and, in doing so, lay bare three defects in the Board's reasoning.

a) Whether Losses Must be Tied to Convicted Conduct

One way that loss determinations under the Guidelines and the INA diverge is that they train on different kinds of conduct. For sentencing purposes, a district court may review losses resulting from any "relevant conduct," which "need not be admitted, charged in the indictment, or proven to a jury." *Alaka v. Att'y Gen.*, 456 F.3d 88, 108 (3d Cir. 2006); *see* U.S.S.G. § 1b1.3(a); *United States v. Payano*, 930 F.3d 186, 198 (3d Cir. 2019) ("[A] sentencing court possesses great discretion in the conduct it may consider . . . even if the conduct was not proven at trial[.]"). For immigration purposes, however, the agency must "focus narrowly on the loss amounts that are particularly tethered to convicted counts."[11] *Alaka*, 456 F.3d at 107; *see Knutsen v. Gonzales*, 429 F.3d 733, 736–37 (7th Cir. 2005) (explaining that the "plain language" of the INA "forecloses inclusion of losses stemming from unconvicted offenses"). And even then, in contrast to the Guidelines, see *Singh*, 677 F.3d at 511–12, the amounts must reflect actual and not merely intended losses, at least in the case

[11] To be clear, while the Board cannot consider losses stemming from unconvicted conduct when analyzing § 1101(a)(43)(M)(i), our decision today does not prevent the agency from reviewing that conduct when deciding whether to grant discretionary relief, such as cancellation of removal, see *id*. § 1229b(b)(1). *See In re C-V-T-*, 22 I. & N. Dec. 7, 11–12 (BIA 1998) (empowering IJs to account for the "nature, recency, and seriousness" of a noncitizen's crimes when determining whether to afford discretionary relief).

of substantive offenses, see Section III.B.2 *infra* (addressing conspiracy and attempt offenses). To visualize the relationship between these standards, imagine two concentric circles: The INA, the inner circle, covers actual losses tied to the convicted conduct itself, while the Guidelines, the outer circle, encompasses both actual and intended losses from convicted conduct and all other related conduct.

This case illustrates that distinction. At its core, the Board's loss analysis centers on the allegations that Rad conspired to "pump" the price of penny stocks by misleading investors and then "dump" his shares of those stocks at a profit. A.R. 4–5. But most of the indictment's counts feature CAN-SPAM Act charges, and only one, the conspiracy-to-commit-securities-fraud count, alleges that Rad duped investors into buying stocks that later declined in value. And, although the Board presumed Rad was guilty of securities fraud, the verdict form reveals that the jury declined to convict Rad of that charge. Thus, the agency's loss analysis rests on the mistaken assumption that the District Court found Rad guilty of securities fraud, and that victim losses are attributable to him on that basis.

That error would make little difference if the Guidelines governed. In that scenario, the Board could easily characterize the unconvicted aspects of the pump-and-dump scheme as "related" to Rad's CAN-SPAM Act convictions. *Id*.; *see* U.S.S.G. § 1B1.3(a) (defining as related conduct "all acts and omissions . . . by the defendant . . . that occurred during the commission of the defense of conviction"). Under the INA,

however, the agency can only consider losses stemming from the pump-and-dump scheme if that scheme embodies the "specific way" Rad committed the CAN-SPAM Act conspiracy counts, *Nijhawan*, 557 U.S. at 34, or if a "direct link" ties the conduct underlying those counts to investors' losses, *Fan Wang*, 898 F.3d at 351. It could be the case, for example, that Rad's use of false headers and domain names enabled him to reach more investors or earn greater trust from the investors he did reach, prompting them to purchase stocks that ultimately declined in value. Whatever the connection between Rad's CAN-SPAM Act offenses and investor losses, however, the challenged order omits any discussion of it. Whether any victim losses are "particularly tethered" to Rad's convictions is thus an issue we must leave for the BIA to resolve in the first instance. *Alaka*, 456 F.3d at 107.

b) How an Offender's Gains Affect the Loss Calculation

Another difference between sentencing hearings and immigration proceedings is the role an offender's gains play in the loss determination. The Guidelines make clear that when "there is a loss but it reasonably cannot be determined," a district court may increase the offense level based on "the gain that resulted from the offense." U.S.S.G. § 2B1.1, cmt. n.3(b). The relevant INA section, by contrast, trains on "loss to the victim or victims," 8 U.S.C. § 1101(a)(43)(M)(i), and makes

no provision for the agency to treat gains and losses as interchangeable.[12]

This is not to say that the Board may never use an offender's gains to support the loss element. In many cases, a defendant's earnings will provide powerful circumstantial evidence of victim loss.[13] In a fraud case, for instance, DHS may be able to show the statutory threshold is satisfied by using the defendant's commission percentage to estimate the volume of fraudulent sales. As this example attests, DHS can establish the loss element without specifically identifying a victim or

---

[12] The Board's decision does not purport to interpret the INA's loss element, and, in any event, we refuse to afford *Chevron* deference to unpublished Board decisions. *See Mahn v. Att'y Gen.*, 767 F.3d 170, 173 (3d Cir. 2014) ("We join our sister circuits in concluding that unpublished, single-member B[oard] decisions are not entitled to *Chevron* deference.").

[13] In this respect, the INA resembles a previous version of the Guidelines, which did not authorize courts to treat gains as a substitute for losses. *See United States v. Hoffecker*, 530 F.3d 137, 197 (3d Cir. 2008) ("The court need only make a reasonable estimate of the loss, given the available information.") (quoting U.S.S.G. § 2F1.1, cmt. 8 (1997), a now-deleted subsection). Under that version of the Guidelines, the question was whether "some logical relationship [links] the victim's loss and the defendant's gain so that the latter can reasonably serve as a surrogate for the former." *United States v. Dickler*, 64 F.3d 818, 826 (3d Cir. 1995). We read the INA as requiring the agency to answer a similar question whenever it uses an offender's gains as a proxy for victim losses.

victims; all the statutory text requires is that victims exist, and that they have collectively lost over $10,000. *See* 8 U.S.C. § 1101(a)(43)(M)(i).

What is fatal to the challenged order is not that the agency used gains to estimate losses, but that it simply equated them, without evaluating how, if at all, Rad's earnings relate to investor harms. And, contrary to DHS's suggestion, the District Court's sentencing decision cannot fill the gap left by the agency's missing analysis. Considering that the Guidelines leave open the possibility that the District Court elevated Rad's offense level without calculating the losses attributable to his conduct, and that the Probation Office urged that approach, we have no assurance that the Court found Rad's crimes to have caused over $10,000 in losses. Ultimately, then, the Board's failure to substantiate any relationship between Rad's profits and investors' injuries supplies a second ground on which to disapprove the challenged order.

c) Which Burden of Proof Governs

A third distinction between the Guidelines and the INA is that they articulate different burdens of proof. While a preponderance-of-the-evidence standard applies at sentencing, see *United States v. Fisher*, 502 F.3d 293, 305 (3d Cir. 2007), a clear-and-convincing evidence standard governs removal proceedings, see *Kiareldeen*, 273 F.3d at 553. Given that the District Court analyzed the loss issue under a different and less demanding burden of proof, the agency would have needed to perform an independent review of the evidence to confirm that

Rad's crimes inflicted harm. *See Nijhawan*, 557 U.S. at 42 (directing the Board to "assess findings made at sentencing 'with an eye . . . to the burden of proof of employed'") (quoting *In re Babaisakov*, 24 I. & N. Dec. 306, 319 (2007)). Neither the Board nor the IJ did so. That provides us with yet another reason to reject the agency's loss analysis.

To sum up, whether a victim loss question implicates the Guidelines or the INA has sweeping consequences. It determines whether losses must be tethered to convicted conduct, dictates the role the offender's gains play in the loss calculation, and decides the relevant burden of proof. Yet the challenged order glosses over these differences and instead treats the Guidelines and the INA as coextensive. This error infects almost every aspect of the agency's analysis, from the conduct it examined to the standard it applied. Because we are bound to review what the Board did, not what it might have done, we have no choice but to vacate the challenged order. *See Dia*, 353 F.3d at 241.

2. Why Remand Is Warranted

All that remains is to decide whether to give the Board what would be a third chance to evaluate this element. When an agency has "had two opportunities to address the legal and factual issues" in a case, we normally refuse to "give it a third bite at th[e] apple." *Yusupov v. Att'y Gen.*, 650 F.3d 968, 993 (3d Cir. 2011) (quoting *Zhu v. Gonzales*, 493 F.3d 588, 602 (5th Cir. 2007)). That is especially true where, as here, the Board failed to meaningfully revise its reasoning after the first

remand. Though DHS's motion to remand highlighted controlling cases that the initial order overlooked, including an opinion that emphasizes the disjunction between the INA and the Guidelines, see *Singh*, 677 F.3d at 511, the agency persisted in ignoring those authorities. Should this troubling trend continue, we will have no choice but to eschew remand and instead direct the Board to reject DHS's request to remove Rad. *See, e.g.*, *Yusupov*, 650 F.3d at 993.

In this case, however, we find ourselves compelled to give the Board one last opportunity to review the victim loss element. The Supreme Court announced in *Florida Power & Light Co. v. Lorion* that "if [an] agency has not considered all relevant factors . . . the proper course, except in rare circumstances, is to remand to the agency for additional investigation or explanation." 470 U.S. 729, 744 (1985). Thus, we remand at this point not to permit the Board to retread the evidence and arguments it has twice encountered, but to allow it to examine an avenue for attributing victim losses that it never considered. *See Kang v. Att'y Gen.*, 611 F.3d 157, 168 (3d Cir. 2010) (explaining that we decline to remand only when "application of the correct legal principles to the record could lead . . . to [a single] conclusion" (emphasis omitted)).

More specifically, Rad's offenses may reflect intended, rather than actual, losses. As discussed above, the jury convicted Rad of conspiracy to violate §§ 1037(a)(3) and (a)(4), not substantive violations of those provisions. That matters because Rad's crimes implicate 8 U.S.C. § 1101(a)(43)(U), which establishes that "an attempt or

conspiracy to commit" an offense under § 1101(a)(43)(M) counts as an aggravated felony. In the past, we have acknowledged that a question exists as to whether "intended loss" may "satisf[y] the loss requirement for attempts or conspiracies to commit a deceit offense under subparagraph (U)," but we have not had occasion to resolve the issue. *Singh*, 677 F.3d at 511 n.7.

Today, we join the Second Circuit, Ninth Circuit, and Board in recognizing that a conspiracy or attempt to commit fraud or deceit involving over $10,000 in intended losses qualifies as an aggravated felony.[14] *See Li v. Ashcroft*, 389 F.3d 892, 896 n.8 (9th Cir. 2004), *overruled on other grounds by Nijhawan*, 557 U.S. 29; *Ljutica v. Holder*, 588 F.3d 119, 125–26 (2d Cir. 2009); *In re S-I-K-*, 24 I. & N. Dec. 324, 327 (BIA 2007). This makes sense both as a textual matter and as a practical one. Read together, subsections M and U define an "offense" as conduct that "involves fraud or deceit in which the loss to the victim . . . exceeds $10,000," and go on to clarify that "an attempt or conspiracy to commit" that "offense" constitutes an aggravated felony. 8 U.S.C.

[14] The Ninth Circuit also suggested that "potential" loss may satisfy 8 U.S.C. § 1101(a)(43)(U). *Li*, 389 F.3d at 896 n.8. Under our precedent, however, a conspiracy must feature "an *intent* to achieve a common illegal goal." *United States v. John-Baptiste*, 747 F.3d 186, 204–05 (3d Cir. 2014) (emphasis added). Thus, a noncitizen cannot "conspir[e] to commit" an offense under § 1101(a)(43)(M)(i) unless he intends to commit a crime that would, if completed, result in over $10,000 in losses. § 1101(a)(43)(U).

§§ 1101(a)(43)(M)(i), (U). It follows that a conspiracy to inflict losses satisfies subsection U, even if it never produces harm. And, because many conspiracies involve no actual losses at all, a contrary conclusion would dramatically limit the scope of subsection U as applied to subsection M—a result Congress is unlikely to have intended. *See United States v. Watkins*, 339 F.3d 167, 178 (3d Cir. 2003) ("A conspiracy charge does not require proof of success in committing the offense[.]").

On remand, the Board must decide whether, in conspiring to violate §§ 1037(a)(3) and (a)(4), Rad intended to cause over $10,000 in investor losses. Perhaps Rad agreed to use false headers and domain names to evade spam filters, reach a larger audience, and induce more investors to purchase stocks he expected to plummet in value. Perhaps Rad meant for the false headers and domain names to confuse investors, prompting them to launch costly investigations. *See, e.g.*, *Tian v. Holder*, 576 F.3d 890, 896 (8th Cir. 2009) (finding that expenses a victim incurred in investigating computer crimes satisfied the INA's $10,000 loss requirement). Or perhaps not. We express no opinion as to the ultimate outcome and leave it to the agency to explore these and other possibilities on remand.

IV. Conclusion

For the foregoing reasons, we grant the petition for review, vacate the Board's removal order, and remand for

further consideration of whether Rad's CAN-SPAM Act convictions reflect over $10,000 in intended losses.