DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 70 December 2022 Number 4

United States Department
of Justice

Executive Office for United
States Attorneys

Washington, D.C. 20530

The Department of Justice Journal
of Federal Law and Practice is
published pursuant to
28 C.F.R. § 0.22(b).

The Department of Justice Journal of
Federal Law and Practice is published
by the Executive Office for United States
Attorneys

Office of Legal Education

1620 Pendleton Street
Columbia, SC 29201

Cite as:

70 DOJ J. FED. L. & PRAC., no. 4, 2022.

Internet Address:

https://www.justice.gov/usao/resources/
journal-of-federal-law-and-practice

Page Intentionally Left Blank

Combatting White-Collar Crime and Fraud

In This Issue

Page Intentionally Left Blank

Introduction

Mandy Riedel
Assistant United States Attorney
White Collar Crime Coordinator
Executive Office for United States Attorneys

Welcome to this exciting edition of the *Department of Justice Journal of Federal Law and Practice*, which focuses on the theories, tools, and tactics that federal prosecutors can use to combat financial crime. These articles were drafted in the wake of the Deputy Attorney General's guidance on corporate crime enforcement. These revisions reinforced the longstanding view that white-collar crime, in particular corporate crime, will "always be a core priority for the Department," with the "first priority" being "to hold accountable the individuals who commit and profit from corporate crime."[1] In March 2022, the Attorney General reiterated this enhanced focus in remarks delivered to the American Bar Association's National Institute on White Collar Crime, where he touted the Department's efforts to enforce individual accountability and ensure the impartial application of the law.[2] Other core Department priorities have also included health-care fraud, COVID-19 fraud, and elder justice initiatives, all of which may fall under the umbrella of white-collar crime.

These crimes are frequently, and perhaps inevitably, complex and sweeping in scope, ranging from global securities and accounting schemes by multinationals to a singular act of deception against an elder by an individual wrongdoer. A common thread binding these crimes lies in the often latent or even invisible effects on the victims; rarely, if ever, is white-collar crime victimless. A company that engages in overseas corruption by bribing a foreign official or illegally gaming the U.S. procurement process hurts others by engaging in anti-competitive behavior, lowering the ethical standards by which all U.S. companies should act, and impairing the efficient functioning of the marketplace. An individual who illicitly exploits innovations in digital assets and blockchain technology brings disrepute to genuine innovators who want to use these developments for the public good and to advance the U.S. economy. As the Attorney General stated, white-collar crimes "weaken[] our economic institutions by undermining public trust in the fairness of those institutions," while failing to prosecute such crimes "weakens our democratic institutions by undermining public trust in the rule of law."[3]

---

1. Lisa O. Monaco, U.S. Dep't of Just., Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group (2022).
2. Merrick B. Garland, U.S. Att'y Gen., U.S. Dep't of Just., Remarks to the ABA Institute on White Collar Crime (Mar. 3, 2022).
3. *Id.*

Fortunately, Department prosecutors have the tools and know-how to act on these priorities. And the articles in this issue not only reflect these abilities but also provide sound, practical tips for federal prosecutors to consider when moving on a white-collar case. Despite the factually compelling narratives that federal prosecutors can employ when making their case in court, equally if not more important is their skillful use and knowledge of legal tools and tactics. Knowing how and when the crime–fraud exception applies to attorney–client privilege and work product protections, how and when to deploy filter teams as investigations become more sensitive and multi-faceted, and how and when a fraud scheme has occurred are just a few examples of the tools, tactics, and concepts that white-collar crime prosecutors must be aware of.

The articles contained in this issue of the *Journal* provide just this type of practical guidance for economic crimes prosecutors. Appellate Counsel Andrew Laing begins by analyzing what constitutes money or property fraud under the relevant statutes designed to combat white-collar crime. Special Matters Unit Chief John Kosmidis and Litigation Unit Chief Jerrob Duffy discuss the circumstances under which the crime–fraud exception to the attorney–client privilege and work product doctrine may apply in order to discover potentially relevant communications. Trial Attorney Lindita Ciko Torza and Special Matters Unit Assistant Chief Timothy Coley then describe the role of filter teams, in particular the Special Matters Unit, in avoiding complications arising from legal ethics and various privilege issues. With this essential conceptual and practical information in mind, we next dive into an assortment of substantive white-collar crime issues. Former Acting Principal Deputy Chief of the Market Integrity and Major Frauds Unit Justin Weitz and Trial Attorney Jennifer Farer analyze the tools, cases, and theories of liability for securities and commodities fraud that can also apply in a civil enforcement context. AUSA David Salem and FCPA Unit Assistant Chief Derek Ettinger give us insights into and lessons learned from a Foreign Corrupt Practices Act case that they recently jointly (and successfully) prosecuted. AUSA Timothy Vavricek sheds light on an important but less publicized type of white-collar crime involving the use of power-of-attorney fraud to scheme and abuse the elderly. Trial Attorneys Philip Andriole and Chris Maietta go global by detailing the work and mission of a (relatively) new interagency group called the Procurement Collusion Strike Force that focuses on antitrust and wire/mail fraud schemes. U.S. Digital Currency Counsel Sanjeev Bhasker, AUSA Alexandra Comolli, and Trial Attorney Olivia Zhu round up our discussion by taking us into the digital world, which the criminal underworld is exploiting at an incredibly rapid pace, and describing how to apply traditional legal tools and tactics to digital asset investigations and prosecutions.

The authors' contributions in this issue represent the Department's commitment to use all the resources and knowledge at its disposal to combat white-collar crime and fraud. They further signify how the Department adeptly responds both to evolving older or to entirely new developments in the fraud and corruption space. I therefore first want to thank our authors not only for

their contributions here but also to the Department and its mission of delivering justice for the public good. I also want to thank all those who worked behind the scenes with editing, reviewing, publishing, and disseminating the incredible wealth of information held in this issue of the *Journal*. I trust that you will find this information as interesting and helpful as I have and encourage all Department attorneys to consider contributing to the *Journal*.

AUSA Mandy Riedel is currently the White Collar Crimes Coordinator for the Executive Office for United States Attorneys. In this position, Mandy is the Department's subject matter expert for white collar crimes, the national COVID-19 fraud coordinator, and the national elder justice coordinator. She oversees nationwide training and policy on financial crimes for the Department. This includes government program fraud, investment and financial fraud, and money laundering, among other things. Mandy has been a federal prosecutor for more than 18 years, primarily focusing on prosecuting white-collar crime. She started her prosecutorial career at the Department's Criminal Division, Fraud Section, in Washington, D.C. in 2004. After more than four years, she joined the U.S. Attorney's Office for the Middle District of Florida. She has handled numerous complex investigations, prosecutions, and trials, including multi-week trials involving electronic evidence, foreign evidence, and complex financial evidence. Mandy has developed expertise in prosecuting financial fraud, identity theft crimes, and victim-related crimes including child exploitation, human trafficking, and civil rights. Before working for EOUSA in her current role, Mandy served the Middle District of Florida in multiple supervisory capacities including as the Deputy Criminal Chief, Acting Chief of the Special Victims Section, and Senior Litigation Counsel.

Page Intentionally Left Blank

Water Under the Bridge: Assessing the Effect of *Kelly v. United States*

Andrew W. Laing
Appellate Counsel
Fraud Section
Criminal Division

I. *Kelly* reminds us that "not every corrupt act . . . is a federal crime"

The Supreme Court's decision in *Kelly v. United States*[1] is the latest in a line of cases emphasizing the boundaries of the money or property fraud statutes. Its ripple effects are being felt in fraud cases across the country—civil and criminal, large and small. This article seeks to put those effects in perspective, beginning with a recapitulation of *Kelly*'s facts and a discussion of what the opinion did and did not hold.

A. The facts and holdings of *Kelly*: a refresher

"Bridgegate," the facts of which many are by now familiar, remains one of the most breathtakingly brazen acts of political vengeance in living memory. In 2013, the Governor of New Jersey was running for re election. In an effort "to notch a large, bipartisan victory," his Deputy Chief of Staff "avidly courted Democratic mayors for their endorsements," including the Mayor of Fort Lee.[2] After the Mayor informed the Deputy Chief of Staff's office that he would not be endorsing the Governor, the Deputy Chief of Staff and two New Jersey-aligned officials at the Port Authority of New York and New Jersey (Port Authority) concocted a plan for vengeance. By reducing from three to one the number of toll lanes on the George Washington Bridge reserved for New York City-bound Fort Lee traffic, they would "create a traffic jam that would punish" the Mayor and "send him a message."[3]

The success of this plan depended on using Port Authority resources, which the conspirators caused to be expended in two ways. First, the three conspirators agreed to spin a cover story to explain the lane change, falsely claiming that it "was part of a traffic study, intended to assess whether to retain the dedicated Fort Lee lanes in the future."[4] To make this ruse more persuasive,

1. 140 S. Ct. 1565 (2020).
2. *Id.* at 1569.
3. *Id.* (internal quotation marks and brackets omitted).
4. *Id.*

one of the conspirators directed Port Authority engineers to collect data on traffic delays resulting from the lane-closure scheme—data collection that required engineers' "valuable time" but ultimately "was to no practical effect."[5] Second, the conspirators agreed to cause the Port Authority to pay for the extra "on call" toll collectors who would be required to be on standby in order to implement the plan.[6]

The conspirators executed their plan on September 9, 2013—the already traffic-heavy first day of school—and it was immediately, spectacularly successful.[7] Fort Lee's "streets came to a standstill," and "the traffic rivaled that of 9/11," when the George Washington Bridge shut down completely. School buses stood motionless for hours, and vital emergency services were delayed.[8] The conspirators nonetheless maintained "radio silence," ignored the Mayor's panicked entreaties, and "merrily kept the lane realignment in place." Three days later, the Port Authority's Executive Director found out and immediately put an end to it.[9]

Swift backlash, a New Jersey State Assembly investigation, and a federal criminal investigation ensued.[10] Ultimately, one of the three conspirators became a cooperating witness, while the other two were convicted following a jury trial of conspiracy to obtain by fraud, knowingly convert, or intentionally misapply property of an organization receiving federal benefits, in violation of 18 U.S.C. § 371; the substantive object of that conspiracy, in violation of 18 U.S.C. § 666(a)(1)(A); conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; and wire fraud, in violation of 18 U.S.C. § 1343.[11]

A unanimous panel of the Third Circuit affirmed in relevant part.[12] Before the district court, the defendants "principally argue[d] they could not have committed fraud because [the Port Authority official defendant] possessed the unilateral authority to control traffic patterns at Port Authority facilities and

---

5. *Id.* at 1570.
6. *Id.* at 1570 ("Ordinarily, if a toll collector on a Fort Lee lane has to take a break, he closes his booth, and drivers use one of the other two lanes. Under the one-lane plan, of course, that would be impossible. So the Bridge manager told [a conspirator] that to make the scheme work, an extra toll collector would always have to be on call to relieve the regular collector when he went on break." (internal quotation marks omitted)).
7. *Id.*
8. *Id.*
9. *Id.* (internal quotation marks omitted).
10. United States v. Baroni, 909 F.3d 550, 559 (3d Cir. 2018), *rev'd sub nom. Kelly*, 140 S. Ct. 1565.
11. *Baroni,* 909 F.3d at 556 n.2, 560. The defendants were also convicted on conspiracy and substantive civil rights counts under 18 U.S.C. §§ 241–42, in connection with their efforts to "interfere with the localized travel rights of the residents of Fort Lee." *Id.* at 585. Following a lengthy discussion (fascinating in its own right but beyond the scope of this article), the Third Circuit concluded that the right to intrastate travel was not clearly established and reversed those convictions. *Id.* at 585–88. The civil rights counts were not at issue before the Supreme Court.
12. *Id.* at 588–89.

to marshal the resources necessary to implement his decisions." In other words, an official cannot defraud an entity of something he possesses the unilateral authority to control. The court observed that the defendants did not even make sufficiency arguments regarding the nature of "the property at issue."[13] The court of appeals nonetheless reached and rejected the defendants' argument that "they did not deprive the Port Authority of any tangible property."[14] First, the court explained that the evidence at trial showed that the defendants obtained, "at a minimum, public employees' labor" in the form of overtime toll booth workers and traffic engineers.[15] Second, the court held in the alternative that the defendants had also deprived the Port Authority of its "right to control" the George Washington Bridge itself, explaining that "[t]he Port Authority's physical property—the bridge's lanes and toll booths—are revenue-generating assets" and that the Port Authority had "an unquestionable property interest in the bridge's exclusive operation," which the defendants "usurp[ed]."[16]

The Supreme Court disagreed on both fronts. The Court began its discussion by emphasizing that "[t]he Government in this case needed to prove *property* fraud," explaining that "[t]he wire fraud statute . . . prohibits only deceptive 'schemes to deprive [the victim of] money or property'" and that, "[s]imilarly, the federal-program fraud statute bars 'obtain[ing] by fraud' the 'property' (including money) of a federally funded program or entity like the Port Authority."[17] Quoting liberally from its earlier decision in *McNally v. United States*, the Court repeated its admonition that the fraud statutes are "'limited in scope to the protection of property rights'" and, as such, "leave[] much public corruption to the States (or their electorates) to rectify."[18]

The Court then addressed and rejected each of the two theories of property deprivation that the government had advanced and that the Third Circuit had blessed: first, that the defendants "sought to commandeer part of the Bridge itself by taking control of its physical lanes"; and second, that the defendants "aimed to deprive the Port Authority of the costs of compensating the traffic engineers and back-up toll collectors who performed work relating to the

---

13. *Id.* at 562–64.
14. *Id.* (internal quotation marks omitted).
15. *Id.* at 565–66.
16. *Id.* at 566–68. The Second Circuit has discussed the "right to control" theory of property fraud in greater depth on several occasions, including in a case now pending before the Supreme Court. United States v. Percoco, 13 F.4th 158, 170 (2d Cir. 2021), *cert. granted*, 2022 WL 2347617 (2022).
17. Kelly v. United States, 140 S. Ct. 1565, 1571 (2020) (quoting McNally v. United States, 483 U.S. 350, 356 (1987), and 18 U.S.C. § 666(a)(1)(A)) (brackets in internal quotations in *Kelly*). Of course, Section 666 does not *only* prohibit "obtain[ing property] by fraud"; it also criminalizes knowingly converting or "intentionally misappl[ying]" property. 18 U.S.C. § 666(a)(1)(A). The Court did not discuss these alternative bases for liability.
18. *Kelly*, 140 S. Ct. at 1571 (quoting *McNally*, 483 U.S. at 360).

lane realignment."[19] With respect to the first theory—commandeering the lanes—the Court began its analysis with its decision in *Cleveland v. United States*, in which the Court rejected the government's claim that the defendant's "fraud aimed to deprive [Louisiana] of property by altering its licensing decisions" in the form of its allocation of yet-to-be-issued gaming licenses.[20] The Court explained that a government's "'intangible rights of allocation, exclusion, and control'—its prerogatives over who should get a benefit and who should not—do 'not create a property interest,'" but rather implicate "the State's 'sovereign power to regulate.'"[21] The Court applied that rationale to the allocation of the George Washington Bridge's toll lanes, reasoning that the defendants did not "take the lanes from the Government" but rather "exercised the regulatory rights of allocation, exclusion, and control—deciding that drivers from Fort Lee should get two fewer lanes while drivers from nearby highways should get two more."[22]

With respect to the second theory—Port Authority employees' time and labor—the Court acknowledged that "[a] government's right to its employees' time and labor . . . can undergird a property fraud prosecution," but it stressed that "that property must play more than some bit part in a scheme: It must be an 'object of the fraud.'"[23] Again comparing the facts in *Cleveland*, the Court explained that, although the frauds in *Kelly* and in *Cleveland* both "doubtless imposed costs calculable in employee time," "[t]he object of the scheme was never to get the employees' labor"; "said another way, the labor costs were an incidental (even if foreseen) byproduct of [the defendants'] regulatory object."[24] Having found no cognizable property interest that was an "object" of the defendants' fraud scheme, and emphasizing that "not every corrupt act by state or local officials is a federal crime," the Court reversed.[25]

B. What *Kelly* did and did not do

Kelly is another in a line of Supreme Court cases fencing in the money or property fraud statutes.[26] But it is important to emphasize the boundaries of its holdings. *Kelly*, by its terms, makes very clear that its exclusive focus is "*property* fraud," not "bribes or kickbacks (not at issue here)," not other aspects of 18 U.S.C. § 666 (like misapplication of property as opposed to obtaining property by fraud), and not similar but differently structured statutes

19. *Id.* at 1572 (cleaned up).
20. *Id.* at 1572 (quoting Cleveland v. United States, 531 U.S. 12, 23 (2000)).
21. *Id.*
22. *Id.* at 1573 (internal quotation marks omitted).
23. *Id.* (quoting Pasquantino v. United States, 544 U.S. 349, 355 (2005)).
24. *Id.* at 1573–74.
25. *Id.* at 1574.
26. *See, e.g.*, Skilling v. United States, 561 U.S. 358, 405, 410 (2010) (adopting "a limiting construction" of 18 U.S.C. § 1346, confining honest services fraud to schemes involving bribes or kickbacks); Cleveland v. United States, 531 U.S. 12, 26 (2000); McNally v. United States, 483 U.S. 350, 356–58 (1987).

like 18 U.S.C. § 1348, which criminalizes securities fraud.[27] Although *Kelly* brought the distinction between property and governmental regulatory interests to a new context—from the intangible yet-to-be-issued gaming licenses in *Cleveland* to physical, tangible lanes on a bridge) —it relied exclusively on existing precedent interpreting the fraud statutes in doing so.[28] *Kelly* also does not disturb or even mention the Court's decades-old holding that the "property" at issue in a fraud case need not be tangible.[29]

II. *Kelly*'s limited effect

What, then, have been the effects of *Kelly* on the sprawling universe of money or property fraud prosecutions? Although *Kelly* was decided only two years ago—the blink of an eye in federal white-collar litigation—the case law interpreting *Kelly* has reinforced the message that the decision, while significant, is merely a reiteration of settled law. Below, this article examines a selection of cases that have grappled with the two principles that *Kelly* rearticulates: that regulatory power is not property, and that property must be an object of a money or property fraud scheme.

A. "Regulatory power" is not "property"

Kelly makes plain that a fraud scheme whose object is a government's "regulatory power," without more, cannot undergird a property fraud conviction. This is so even when the regulatory power at issue pertains to the government's rights of "allocation, exclusion, and control" over a piece of physical property like a bridge.[30] Unsurprisingly, defendants in several post-*Kelly* cases have sought to use *Kelly* as a shield. These cases involved property that happens to be in the hands of governments or involve government regulation that is a part of, but not the sole (or even an) object of the fraud. Courts have largely

27. *Kelly*, 140 S. Ct. at 1571–72; *see* United States v. Ramsey, No. 19-cr-268, 2021 WL 4244284, at *3–4 (E.D. Pa. Sept. 27, 2021) (observing that § 1348 "differs significantly from the mail and wire fraud statutes," explaining that § 1348(1) "makes no mention of money or property" and that "the language that *Kelly* construed" in § 1343 "simply does not exist in § 1348(1)").

28. *See, e.g.*, *In re* Ranbaxy Generic Drug Application Antitrust Litig., No. 19-md-2878, 2021 WL 5493675, at *3 (D. Mass. Nov. 22, 2021) (rejecting *Kelly*-based argument that the court should "reconsider its determination" that plaintiffs adequately alleged mail and/or wire fraud as civil RICO predicates, explaining that "*Kelly* is a straightforward application of the holding in *Cleveland*," which the court had already determined did not bar claims that defendant's scheme targeted "not simply the government's regulatory choice but rather the property rights implicated by that choice"); United States v. Khoury, No. 20-cr-10177, 2021 WL 2784835, at *3 (D. Mass. July 2, 2021) (explaining that "*Kelly* merely affirmed the holding and other courts' reading of *Cleveland*" regarding regulatory interests and "did not alter the Court's precedent regarding what constitutes property").

29. Carpenter v. United States, 484 U.S. 19, 25 (1987) ("[Confidential business information's] intangible nature does not make it any less 'property' protected by the mail and wire fraud statutes.").

30. *Kelly*, 140 S. Ct. at 1572–73 (internal quotation marks omitted).

resisted those efforts.

For example, in *United States v. Spirito*, the Fourth Circuit addressed a defendant's section 666(a)(1)(A) misapplication convictions involving property in the hands of a governmental entity.[31] The defendant, an airport executive, improperly used government funds and airport revenue to provide collateral for a private bank loan to a startup airline that quickly failed, resulting in the loss of the collateral.[32] Among many other things, the defendant argued on appeal that his section 666 convictions were infirm because, under *Kelly*, "he made a mere regulatory decision regarding the funds and, even if the decision was bad or made for sinister reasons, it does not amount to the 'misapplication' of property."[33] Rather, the defendant contended that he merely "exercise[d] his right to allocate airport funds among airport uses, even if such allocations broke the rules."[34] Not so, the court replied: The defendant "did not use his regulatory power to *allocate* airport funds 'among airport uses'"; rather, "[h]e used his regulatory power to *pledge* airport funds to a private entity . . . for the exclusive benefit of another private entity . . . . Unlike *Kelly*, which involved the use of regulatory power for political retribution, the object of the crime here was property and the goal was to misapply property owned by the airport."[35] In other words, *Kelly* does not shield a defendant who illegitimately misapplies government property and cloaks that misapplication in the language of regulatory power.

Several other post-*Kelly* cases, including in civil contexts, have grappled with the more difficult distinction between schemes whose *object* is regulatory power on the one hand and schemes that *involve* regulation but have a valid money or property object on the other. After all, it is easy to imagine a fraud scheme that depends on deceiving a regulator to obtain approval for a product—approval that is, standing alone, a non-property regulatory interest—but whose ultimate object is consumers' money, which is unquestionably a property interest. For instance, in a civil Racketeer Influenced and Corrupt Organizations Act (RICO) case involving e-cigarette regulation, a district court distinguished the facts of *Kelly* from the scheme at issue there. The court explained that, although the defendants "allegedly lull[ed] Congressional legislators and the regulators at the FDA into inaction, or more limited action, to allow their products to remain on the market," the object of the scheme "was to secure the money and property of the end consumers, in particular the new and youth users who were not previously addicted to nicotine."[36] In other words, a fraud scheme whose sole object is "lulling" legislators and regulators targets only a regulatory interest and cannot be characterized as mail or wire fraud. On

31. 36 F.4th 191 (4th Cir. 2022).
32. *Id.* at 194–97.
33. *Id.* at 201.
34. *Id.* (cleaned up).
35. *Id.* at 202 (emphases added).
36. *In re* JUUL Labs, Inc., Mktg., Sales Practices, & Prods. Liab. Litig., 497 F. Supp. 3d 552, 614–15 (N.D. Cal. 2020).

the other hand, a scheme that depends on regulatory manipulation but whose ultimate object is money can.

More recently decided cases provide additional illustrations of this principle. A magistrate judge in *United States v. Dingle* recommended denying a defendant's motion to dismiss an indictment charging wire fraud in connection with an alleged scheme to obtain "small business and veteran-owned business certifications."[37] The judge agreed with the defendant that "[t]he issuance of licenses alone . . . does not implicate a property right," but nonetheless recommended denying the motion.[38] The judge reasoned that "the scheme alleged here involved more than a regulatory crime of defrauding the Government out of licenses"; instead, "[t]he licenses were just the means to an end," namely hundreds of millions of dollars in federal contracts to which the defendants were not entitled.[39]

Most recently, in the context of product liability litigation involving airbags, a district court addressed and rejected a similar argument that, in light of *Kelly*, airbag manufacturers' statements to a regulator "are 'nonactionable' because 'they were not made to obtain money or property.'"[40] The district court brushed aside the defendants' reliance on *Kelly* as "unpersuasive."[41] It explained that, in the case before it, the defendants "allegedly effected a scheme to defraud with the object of depriving consumers of money by selling them defective vehicles worth less than they paid. Although [they] allegedly furthered this scheme by making fraudulent statements to a regulatory agency, that was not their primary, alleged purpose."[42]

These cases illustrate that, although *Kelly* offers additional context for *Cleveland*'s holding that regulatory power by itself is not property, *Kelly* does not eliminate liability for fraud schemes that *involve* regulatory power, either as an arguable aspect of a government-employee defendant's job (as in *Spirito*) or as a means to consumers' money or property ends (as in the other cases discussed above).[43]

---

37. United States v. Dingle, No. 19-cr-215, 2021 WL 1015853, at *1 (W.D. Mo. Feb. 3, 2021).
38. *Id.* at *1.
39. *Id.* at *3; *see also* United States v. Dingle, No. 4:19-cr-215, 2021 WL 982327 (W.D. Mo. Mar. 16, 2021) (adopting report and recommendation and denying motion to dismiss).
40. *In re* ZF-TRW Airbag Control Prods. Liab. Litig., No. 2:19-ml-2905, 2022 WL 522484, at *56 (C.D. Cal. Feb. 9, 2022).
41. *Id.*
42. *Id.*
43. Note that a scheme involving deception directed solely at a regulator in order to obtain property solely in the hands of a third party implicates the question whether the fraud statutes include a so-called "convergence" requirement (that is, a requirement that the party deceived be the same as the party deprived of property). As the First Circuit put it in rejecting such a requirement, "[i]f . . . the role of a government regulator is to protect the monetary interests of others, a scheme to mislead the regulator in order to get at the protected funds will affect 'property rights' as required in *McNally*." United States v. Christopher, 142 F.3d 46, 54 (1st Cir. 1998); *see also*

B. Property "must be an 'object of the fraud'"

Kelly also tells us that a fraud scheme must have money or property as an object: "[A] property fraud conviction cannot stand when the loss to the victim is only an incidental byproduct of the scheme."[44] As the cases discussed below vividly illustrate, property need not be *the sole* object of the fraud—it need just be *an* object of the fraud.

The Second Circuit discussed this issue in depth in *United States v. Gatto*.[45] In that case, several defendants

> were convicted of engaging in a scheme to defraud three universities by paying tens of thousands of dollars to the families of high school basketball players to induce them to attend the universities, which were sponsored by Adidas, the sports apparel company, and covering up the payments so that the recruits could certify to the universities that they had complied with rules of the National Collegiate Athletic Association (the "NCAA") barring student-athletes and recruits from being paid.[46]

On appeal, they argued that the evidence failed to show that they defrauded the universities of anything at all—indeed, they argued that their actions helped the universities by driving top-tier recruits to their basketball teams.[47] So what, if anything, was a valid property object of their fraud? The court concluded that the evidence showed that the universities' "athletic-based aid," undoubtedly a property interest, was an object of the fraud.[48] Distinguishing *Kelly*, the court explained that "the loss of property—the Universities' funds set aside for financial aid—was at the heart of" the scheme; indeed, "the scheme *depended* on the Universities awarding ineligible student-athletes" (ineligible because of the under-the-table payments they accepted) "athletic-based aid."[49] "Unlike in *Kelly*," the court reasoned, "depriving Universities of athletic-based aid was at the *center* of the plan."[50] Significantly, the court acknowledged and did not dispute the defendants' assertion that another object of their scheme was to "lur[e] the best basketball players to Adidas-sponsored schools to better market their brand," but it emphasized the irrelevance of that claim: "Defendants may have had multiple objectives, but property need only be '*an* object' of their scheme, not the sole or primary goal."[51]

United States v. Greenberg, 835 F.3d 295, 306 n.16 (2d Cir. 2016) (joining "at least four sister circuits" in rejecting convergence requirement, and collecting cases).

44. Kelly v. United States, 140 S. Ct. 1565, 1573 (2020).
45. United States v. Gatto, 986 F.3d 104 (2d Cir. 2021).
46. *Id.* at 109–10.
47. *Id.* at 110.
48. *Id.* at 115.
49. *Id.* at 116 (emphasis added).
50. *Id.*
51. *Id.* (quoting Kelly v. United States, 140 S. Ct. 1565, 1572 (2020)) (emphasis added by *Gatto*) (citation omitted).

The Seventh Circuit came to a similar conclusion in *United States v. Shelton*.[52] There, following a lengthy discussion of complex Fourth Amendment issues that ultimately required vacatur and remand, the court addressed whether the defendants had properly been prosecuted for conspiracy to commit wire fraud in connection with a scheme to "use[] public employees and Township resources (such as computers, printers and storage space) to run campaign fundraisers and other campaign activities during regular work hours while paying those employees with Township funds."[53] After reviewing *Kelly*'s discussion of the principle that a "government's right to its employees' time and labor . . . can undergird a property fraud prosecution,"[54] the Seventh Circuit concluded that "[t]he scheme charged here fits comfortably into the paradigmatic cases that the Court described as legitimate money-and-property wire fraud in *Kelly*."[55] The court explained, "[i]f the object of the charged scheme . . . was to obtain the services of on-the-clock government employees to run political campaigns . . . , then the labor costs of this plan were not a byproduct of the scheme; they were *the object* of the scheme."[56] Although the campaign work "also involved a possible kickback scheme," that did not matter to the court's analysis as to the fraud scheme, which, the court concluded, had a valid property object.[57]

Two district court cases further illustrate the principle that fraud schemes can (and often do) have multiple objects, but it is enough for money or property to be at least one of those objects. In *United States v. Porat*, the district court denied the defendant's motion for a judgment of acquittal under Rule 29 of the Federal Rules of Criminal Procedure following his wire fraud trial in connection with his scheme to boost his business school's *U.S. News & World Report* ranking.[58] The court emphasized that *Kelly* made clear that money or property need only be an object of a fraud scheme,[59] and it concluded that at least an object of the defendant's scheme was indeed money. Distinguishing *Kelly*, the court explained—

> It is not plausible to describe taking money from students, applicants and donors as an incidental byproduct of [the defendant's] efforts to secure higher rankings through fraud. [His] efforts did not end when *U.S. News* released its rankings. Once he had them in hand, he worked hard to turn those rankings into money by marketing them . . . . The jury naturally concluded the money higher

52. United States v. Shelton, 997 F.3d 749 (7th Cir. 2021).
53. *Id.* at 774.
54. *Kelly*, 140 S. Ct. at 1573.
55. *Shelton*, 997 F.3d at 774–75.
56. *Id.* at 775 (emphasis added).
57. *Id.*
58. United States v. Porat, No. 21-170, 2022 WL 685686, at *1 (E.D. Pa. Mar. 8, 2022).
59. *Id.* at *25 (rejecting an argument that the jury instruction was erroneous because "it used the indefinite article 'an' rather than the definite article 'the'").

> rankings could bring to the school, not the ranking[s] themselves, was [the defendant's] object.[60]

Along similar lines, a district court denied a defendant's motion to dismiss the indictment in a wire fraud case in *United States v. Sullivan*.[61] In that case, the indictment alleged that the defendant, formerly Uber's Chief Security Officer, learned that hackers had gained unauthorized access to Uber's data.[62] Despite the company's legal obligation to notify affected drivers of the breach, the defendant arranged a cover-up.[63] In moving to dismiss the indictment, the defendant argued in part "that the wire fraud charges should be dismissed because they do not adequately allege that obtaining money or property (i.e., [drivers'] service fees) from the alleged victims (the Uber drivers) was more than an incidental byproduct of his alleged efforts to conceal the data breach."[64] After reviewing *Kelly*, the district court rejected the defendant's argument, concluding that the indictment sufficiently alleged that an object of the defendant's "scheme was to obtain the drivers' service fees."[65] As the district court and the government acknowledged, "[t]here may have been *other* objectives," such as "to protect [the defendant's] own professional or personal reputation," or "to protect Uber from further scrutiny," but it was enough that "*an* object of the scheme was to deprive Uber drivers of their service fees."[66]

C. Looking ahead

Although *Kelly* was only decided recently, these cases begin to paint a picture of its effect. Again, as the opinion itself makes clear, *Kelly* does not make new law, but it clarifies the nature and scope of "regulatory power" that cannot support a fraud conviction. It also clarifies that property must be "an object" of, and not merely incidental to or an implementation cost of, the fraud.[67] Prosecutors handling cases involving government action must take care to remember that governments' regulatory power, even when it involves control of physical assets (that may themselves be "property"), cannot undergird property fraud standing alone. If the fraudulent manipulation of regulatory power is a means to a valid money or property end, it can play a part in a properly charged fraud scheme. And prosecutors must remember that fraud schemes can and often do have multiple objectives. Defendants seeking to enrich themselves may also have professional, reputational, or other types of goals all mixed in their heads at once, but they can still be prosecuted so long as *an* object is money or property.

---

60. *Id.* at *20.
61. United States v. Sullivan, No. 20-cr-337, 2022 WL 2317441 (N.D. Cal. June 28, 2022).
62. *Id.* at *2.
63. *Id.*
64. *Id.*
65. *Id.* at *3.
66. *Id.* at *4 (emphasis added).
67. Kelly v. United States, 140 S. Ct. 1565, 1571–74 (2020).

About the Author

Andrew Laing currently serves as Appellate Counsel within the Litigation Unit of the Fraud Section of the Criminal Division. He joined the Department of Justice through the Attorney General's Honors Program after clerking for the Honorable Patty Shwartz of the U.S. Court of Appeals for the Third Circuit. He has previously served in the Criminal Division's Public Integrity and Appellate Sections.

Page Intentionally Left Blank

Crime–Fraud Litigation in White-Collar Prosecutions

John Kosmidis
Chief, Special Matters Unit
Fraud Section
Criminal Division

Jerrob Duffy
Chief, Litigation Unit
Fraud Section
Criminal Division

I. Introduction

Anyone who has run a filter review as part of a complex white-collar fraud investigation can tell you that targets, subjects, and witnesses frequently communicate with lawyers. These lawyers may be corporate legal counsel or in private practice and may be providing legal advice to corporate employees or specific individuals. The lawyers could be working on matters unrelated to the fraud at issue, unwittingly furthering the fraud, or directly participating in it. Communications with lawyers are potentially covered by attorney–client privilege and attorney work product protections. They are therefore not ordinarily accessible to prosecutors conducting a criminal investigation. Depending on the lawyer's involvement in the fraud, however, these communications could be highly relevant and discoverable if the crime–fraud exception (CFE) to the privilege or protection applies.

A common occurrence in health-care fraud is the use of outside counsel to "whitewash" a fraudulent scheme. Fraudulent actors may design a business model that, in fact, defrauds a health-care provider like Medicare by providing illegal kickbacks for patient referrals. The fraudulent actors will go to outside counsel and provide a false or materially incomplete factual background about the business model that omits the illegal kickback part of the scheme. Based on this false and misleading account, they obtain advice from counsel that the model is lawful. The fraudulent actors will then take that lawyer's stamp of approval and use it to convince business partners, investors, or others that the business practice is lawful, allowing the scheme to continue and grow unabated. The communications with outside counsel are critical for understanding what the target disclosed to counsel to obtain the purported legal advice and demonstrating the target's fraudulent intent.

When applicable, the CFE obviates any privilege that otherwise applies to the communication. When the elements of the CFE are met, it will apply to all communications within the same subject matter, including those obtained

via search warrant, from a voluntary production that implicates the rights of another privilege holder, through an interview with a lawyer or someone with knowledge of privileged material, or to grand jury or trial testimony.

There are multiple considerations to factor in when litigating a CFE motion. Should it be pre- or post-indictment? Do you need to use a filter team? What information should you provide to the court and how? Can and should a motion to the court be filed ex parte? How should you structure the requested relief? Once these questions are resolved, the CFE is a powerful tool for obtaining evidence otherwise unavailable to investigators.

II. Obtaining and handling evidence that may be subject to the CFE

Because the CFE could apply to any potentially privileged material, it can be applied to any source of information over which privilege could be asserted. As noted in the introduction, sources of that material are varied and could include search warrant returns, statements by witnesses, voluntary productions from non-privilege holders that implicate the privilege of another, or testimony. The CFE can also apply to material not yet in the government's possession, including documents or testimony obtained via subpoena.

While a privilege holder bears the burden of asserting privilege, including by providing a privilege log with sufficient specificity that allows a court or a challenging party to understand the nature of the claim asserted, federal prosecutors and investigators must take reasonable steps to avoid exposure to privileged information. Prosecutors and agents should promptly cease review and set aside or return material that they deem to be potentially privileged. One method of segregating such material is to provide it to a filter team and remove the prosecution team's access until the filter review is completed. Filter teams are widely accepted tools to prevent prosecution teams from accessing privileged information.

A filter team should be employed to isolate potentially privileged material in the government's possession. This process includes having a filter team conduct the initial review of documents or testimony that the prosecution team has a reasonable basis to believe may contain otherwise privileged material. As referred to here, a filter team consists of one or more prosecutors not assigned to the case team who will have no role in the prosecution of the case. The "filter prosecutor" should be supported by filter agents and additional personnel as needed and should be available to document, explain, and defend in court any steps or decisions the filter team takes. The filter prosecutor should supervise the segregation of potentially privileged material so that it is unavailable to the prosecution team, communicate with counsel for the privilege holder(s) when necessary, and be prepared to negotiate and litigate privilege issues.

The filter team can identify the potentially privileged material within the data source, segregate it from the prosecution team, release any non-potentially privileged material (allowing the investigation to continue), and address the

potentially privileged material.

A. Search warrant

In white collar criminal investigations, material seized via search warrant is the most common source of obtaining attorney communications. Warrants for stored electronic communications pursuant to 18 U.S.C. § 2703 or obtained via Rule 41 of the Federal Rules of Criminal Procedure present the possibility that attorney–client or other legal communications may be included in the data or materials seized. Collecting such communications is often inadvertent. Prosecutors should think carefully about the potential for seizing privileged material when obtaining such warrants and use a targeted approach and prophylactic measures when appropriate.

After material is seized and determined by the case team to be within the scope of the warrant, a filter team can isolate and segregate potentially privileged material using a variety of techniques, including keyword searches designed to identify such material. Apart from the material released to the prosecution team, the filter team can review the withheld material to identify whether it may be subject to the CFE. It is beneficial if the filter team can become familiar with the prosecution team's theory of the fraud, allowing the filter team to evaluate whether withheld material could be brought to the court and would be impacted by a finding that the CFE applies. It is notable that the filter team can obtain information from the prosecution team to conduct its evaluation but should not disclose potentially privileged material to the prosecution team absent agreement of the privilege holder or court order.

B. Subpoena for documents

The CFE can also be used to obtain otherwise privileged material not yet in the government's possession. For example, if the prosecution team knows that an attorney was involved in furthering a fraud, even unknowingly, the prosecution team can issue subpoenas to that attorney requesting relevant communications subject to applicable approvals.[1.] If the alleged fraud relates to a securities offering where the attorney and client are believed to have conspired to withhold material information from investors, the subpoena can request all communications from the attorney and client regarding the specific securities offering. Depending on the possible number of communications at issue, a more targeted request related to the specific withheld information may be appropriate, if known.

To avoid unintended production of otherwise privileged material, subpoenas issued to attorneys or involving persons known to be represented by counsel should provide specific instructions and detail so that the recipient is aware of the precise nature of material called for in the subpoena. If the recipient or other party seeks to assert a privilege for material called for in the subpoena, the subpoena should also provide directions to the recipient setting out the

1. Subpoenas to attorneys related to representing clients require special authorization. *See* Justice Manual 9-13.410.

requirement to provide a privilege log, including:

- This subpoena is not intended to be a call to produce any material that is subject to a valid claim of attorney–client or other privilege recognized by the courts of the United States.
- To the extent you or some other party may seek to assert a claim of privilege, work product protection, or other legal claim to preclude production of material called for in this subpoena, a privilege log shall be produced.
- Such a log shall set forth the document title, subject matter, author(s), recipients(s), date, transmittal detail (if any), location of author(s) and recipient(s), and an explanation of the claim asserted against production.
- Failure to produce such a log, with sufficient detail to allow a reviewing party or court to assess whether such a claim is valid, may result in waiver of any such claim.

The subpoena recipient, such as a lawyer in the example listed above, will need to provide a privilege log detailing the material that they are claiming to be privileged. At that point, the prosecution team can file a motion to compel compliance with the subpoena, and the CFE litigation can commence.[2.] This motions practice can occur during the grand jury stage or post-indictment, when a trial or hearing subpoena is utilized. As described below, we recommend that these issues be litigated during the grand jury investigation before indictment when possible.

C. Interviews & testimony

In addition to emails and other documents, the CFE may otherwise apply to witness statements and testimony when such a statement may contain privileged information. For example, it can also be used to compel an individual to provide otherwise privileged testimony to a grand jury that would allow active questioning on the topics subject to the CFE. This process requires appropriate approvals and will frequently follow motions practice where the judge presiding over the grand jury has ruled as to the applicability and scope of the CFE to a particular matter.

A filter team can also be employed as a prophylactic measure to conduct interviews where there is reason to believe that the interviewee may make

2. As discussed below, we recommend that in most cases the prosecution team draft and file the motion for a finding that the CFE applies to the documents, communications, or subject matter at issue if the material or information that supports such a finding is available to the prosecution team. An *ex parte* filing by the filter team can then supplement this motion if certain material that would further the claim has been withheld from the prosecution team. In some circumstances, where the filter team is uniquely in possession of the material that supports the CFE finding, the filter team may file the motion.

statements that include potentially privileged material as a means of protecting against inadvertently exposing such information to the prosecution team. When such a process is contemplated, the filter team should work with the prosecution team to prepare for the interview and should carefully approach topics related to attorney–client privilege to avoid receiving privileged responses or information or for which no good-faith basis exists that the CFE will apply. If the interview is with an attorney or someone who will provide mostly or all potentially privileged information, the filter team should conduct the full interview. If the interview is with a non-attorney who will be questioned on largely non-privileged topics, the filter team can conduct the entire interview, or the prosecution team can conduct those portions of the interview not likely to encounter potentially privileged information. If the interview starts to cover potentially privileged topics, the prosecution team can leave or pause the interview, and the filter team should take over.

Following the interview, the filter agent should create a record of the interview, for example an FBI Form-302 or agency Report of Interview, but withhold the record from the prosecution team. That report can then provide support for a motion to authorize disclosing the report to the prosecution team. The interview memorandum should clearly reflect who conducted the interview and who was present during the portions that relate to potentially privileged information.

Like a subpoena for documents, the prosecution team can issue a subpoena to compel a lawyer or witness with otherwise privileged, relevant information to testify in front of the grand jury when there is a good-faith basis to believe that the CFE will apply to the testimony. The testimony should only occur after a court ruling on the applicability or scope of privilege and the CFE, unless the privilege holder has consented in writing.

D. Voluntary productions

In most instances, the material potentially subject to the CFE will come from the privilege holder, either through seizure of communications or a subpoena for the communications at issue. Various persons such as corporate employees or cooperators, however, can possess and produce statements or materials that impact the privilege of others. These communications may also be subject to the CFE. For example, a cooperator could allow the government to image their phone via consent, but the phone might contain communications over which their employer or another party could claim privilege. Another scenario is a cooperator providing communications that could be subject to a common interest privilege claim by another party, because the cooperator was previously part of a joint defense agreement or participated in group meetings involving one or more attorneys. In these scenarios, the cooperator cannot ordinarily waive privilege on behalf of the other privilege holders.

In these situations, a filter team should be used to segregate the potentially privileged information and identify any material subject to the CFE, as it would with search warrant returns. Motions practice or further negotiation

with privilege holders can then follow, and a ruling or clarification can be obtained before the prosecution team is exposed to the information.

III. Litigating the CFE

A. Legal standard

The CFE is a method for courts to balance the sometimes-competing interests of privilege holders and investigators, and the resulting legal standard reflects this. In *United States v. Zolin*, the Supreme Court established a standard for an exception to the attorney–client privilege when otherwise-protected attorney–client communications were connected to an ongoing fraud.[3]

For privilege holders, the attorney–client privilege is a sacrosanct protection. It encourages "full and frank communication between attorneys and their clients and thereby promote[s] broader public interests in the observance of law and administration of justice."[4] Courts are protective of attorney–client communications absent an exception,[5] and government investigators are not entitled to review those communications. If they do so, they are at risk of potential disqualification or, if the review is egregious, dismissal of an indictment.

In setting out revisions to the Principles of Federal Prosecution of Business Organizations, then-Deputy Attorney General Paul McNulty emphasized that the Department agreed with the importance of protecting attorney–client communications:

> The attorney-client privilege is an important part of the legal framework supporting this compliance and accountability. The privilege promotes thorough and complete disclosure from a corporate employee to his attorney and candid advice from legal counsel. It is one of the oldest and most sacrosanct privileges in American law.[6]

These privilege protections, however, come at a cost—they can prevent government investigators from obtaining information that could be relevant to their investigation and otherwise prevent the truth-seeking function of the adversarial system.[7] Accordingly, when a client abuses the system by consulting an attorney for the purpose of furthering criminal or fraudulent activity, the CFE overcomes the application of the attorney–client privilege, and the com-

3. United States v. Zolin, 491 U.S. 554, 561–63 (1989). Additionally, the crime–fraud exception applies to materials for which the work product privilege would otherwise apply. *See In re* Impounded Case (Law Firm), 879 F.2d 1211, 1214 (3d Cir. 1989).
4. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
5. In addition to the CFE, other instances where an attorney–client communication would not garner privilege protection include third-party waiver and that the communication was business advice and not legal advice.
6. Paul J. McNulty, Deputy Att'y Gen., U.S. Dep't of Just., Prepared Remarks at the Lawyers for Civil Justice Membership Conference Regarding the Department's Charging Guidelines in Corporate Fraud Prosecutions (Dec. 12, 2006).
7. *See, e.g.*, *Zolin*, 491 U.S. at 561–63.

munications lose their protected status.[8] Otherwise, justice "would be frustrated if the client used the lawyer's services to further a continuing or future crime."[9]

Zolin established the standard for a successful CFE motion. The party seeking to apply the CFE to overcome the attorney–client privilege must show that "(1) the client was committing or intending to commit a fraud or crime, and (2) the attorney-client communications were in furtherance of that alleged crime or fraud."[10] In *Zolin*, the courts have held that the party asserting the exception must make a prima facie showing of both the above elements.[11]

The prima facie showing is not a high burden. The first element may be satisfied by the allegations of the indictment (a grand jury finding).[12] Broadly, the prima facie showing requires a "reasonable basis" to believe that the client used the lawyer's services to foster a crime or fraud.[13] The reasonable basis standard "affords sufficient predictability for attorneys and clients without providing undue protection to those that seek to abuse the privileges afforded to them."[14]

The court may examine potentially privileged documents to determine if the CFE applies. The party seeking to invoke the exception, however, must make a showing "'of a factual basis adequate to support a good faith belief by a reasonable person,' that *in camera* review of the materials may reveal evidence to establish the claim that the crime fraud exception applies."[15] In essence, the CFE filing must demonstrate, before the court reviewing the underlying communications, that there was fraudulent activity and that the privileged communications were used to further that fraud. The showing for a court to conduct an *in camera* review is even lower than the prima facie standard for establishing that the CFE applies.

Importantly, the CFE only applies to fraudulent activity that is forward looking at the time the communication occurs. The attorney–client privilege "ceas[es] to operate at a certain point, namely, where the desired advice refers

---

8. *Id.*
9. *In re* Grand Jury Proceeding Impounded, 241 F.3d 308, 316 (3d. Cir. 2001) (citing *In re* Grand Jury Proceedings, 604 F.2d 798, 802 (3d. Cir. 1979)).
10. *In re* Grand Jury Subpoena, 223 F.3d 213, 217 (3d Cir. 2000) (citation omitted).
11. *See, e.g., id.*
12. United States v. Gorski, 807 F.3d 451 (1st Cir. 2015).
13. *In re* Grand Jury, 705 F.3d 133, 153 (3d Cir. 2012) ("Where there is a reasonable basis to suspect that the privilege holder was committing or intending to commit a crime or fraud and that the attorney-client communications or attorney work product were used in furtherance of the alleged crime or fraud, this is enough to break the privilege.").
14. *Id.* (explaining that the reasonable basis standard is closest to the Supreme Court's pronouncement that "'there must be something to give colour to the charge' that the attorney-client communication was used in furtherance of a crime or fraud" (quoting Clark v. United States, 289 U.S. 1, 15 (1933))).
15. *In re* Grand Jury Proceedings #5 Empanelled Jan. 28, 2004, 401 F.3d 247, 253 (4th Cir. 2005) (quoting *Zolin*, 491 U.S. at 572).

not to prior wrongdoing, but to *future wrongdoing*."[16] So if a fraudulent actor consults his attorney about an already committed fraud, those communications will likely remain privileged. But if the communications relate to an ongoing or future fraud, the CFE could apply.

The attorney's knowledge of the fraud is not relevant. In many, and perhaps most, instances, the lawyers are not intentional participants in the fraud; the relevant point of view is from the client's side. Is the client committing a fraud? "In determining whether the [crime–fraud] exception is applicable, the client's intention controls and the privilege may be denied even if the lawyer is altogether innocent."[17] "[T]he crime-fraud exception applies even when an attorney is unaware that the client is engaged in or planning a crime."[18]

B. Pre- v. post-indictment considerations

The government has substantial advantages when these issues are litigated pre-indictment, as the litigation with the privilege holder may not involve the targets of the investigation, and information lawfully obtained after a CFE finding may be used in making charging decisions. Further, once a court has made a CFE determination, other avenues of evidence collection can become available to investigators. Separately, once a court makes a CFE finding, the government obtains certainty about allowable areas of inquiry and evidence likely to be admissible at trial.

CFE litigation can take place ex parte, as opposed to on notice to the privilege holder. While courts are often reluctant to make a CFE finding without hearing from the putative privilege holder, in covert matters where a substantial showing can be made to establish the existence of a CFE, courts have issued ex parte CFE orders.

C. The filings

A CFE argument should be broken down into two sections: (1) a description of the fraud at issue and (2) a description of how the privileged communications were used to further that fraud. The mechanics of the filing can vary depending on the status of the case and the material involved, including if a filter team is involved and if the filter team, through its review, has identified material that would support a CFE argument. The prosecution team should handle the description of the fraud at issue based on its investigation.

If pre-indictment, the filing can be made before a grand jury judge or as a miscellaneous filing with a magistrate judge. The filing will require the investigation to be at a stage such that there is sufficient evidence to demonstrate a

16. *Zolin*, 491 U.S. at 562–563 (alteration in original) (citation omitted).
17. *In re* Grand Jury Proceedings, 604 F.2d 798, 802 (3d Cir. 1979).
18. *In re* Grand Jury Investigation, 445 F.3d 266, 279 n.4 (3d Cir. 2006); *see also* United States v. Chen, 99 F.3d 1495, 1504 (9th Cir. 1996) ("The attorney need know nothing about the client's ongoing or planned illicit activity for the [crime–fraud] exception to apply." (quoting *In re* Grand Jury Investigation (The Corporation), 87 F.3d 377, 381–82 (9th Cir. 1996))).

prima facie case that there is an ongoing fraud. This material can come from non-privileged documents, witness statements, or other sources of evidence obtained during the investigation and can be provided to the court as exhibits. As the case is pre-indictment, the filing and underlying material should be done under seal to protect the covert nature of the investigation.

If the investigation is post-indictment, the indictment itself can serve as prima facie evidence of the fraud, with the motion summarizing the fraud as described in the indictment, possibly with supporting material attached as exhibits. That a grand jury has found probable cause for an indictment can be sufficient evidence for a court to find that a fraud has occurred for purposes of prong one of the CFE standard.

After the fraud has been laid out, the argument needs to explain how the privileged relationship was used to further the fraud. The prosecution team can use facts that it is aware of from non-privileged sources to show the connection between the privileged material and the ongoing fraud. For example, the prosecution team may be aware that a securities offering disclosure originally had a provision disclosing a known risk, but after communications with counsel, that risk was removed in material provided to investors defrauded of their investment. The standard for demonstrating that the legal advice furthered the crime is again a prima facie or reasonable basis one and need not be proven conclusively.

The filter team can provide supplemental filings, under seal and ex parte, to the investigating team to support how the privileged material furthered the fraud.

D. Conducting hearings

As with the filings, there is no "right" way to conduct CFE hearings. The prosecution team can be present for any part of the hearing that does not discuss the content of potentially privileged material. The prosecution team is in the best position to describe and argue the merits of the underlying fraud and, if they have the information from non-privileged sources, explain how the attorney communications were made in furtherance of that fraud. If the content of privileged communications is relevant, however, the prosecution team must step out of the courtroom to avoid any potential taint from exposure to it. The court may also seal the courtroom to prevent unauthorized release of protected material.

Additionally, the court may expect testimony in support of the motion and may convene an evidentiary hearing. If so, the same prescriptions should apply. The prosecution team can be involved to the extent that it does not expose them to potentially privileged information. At that point, the filter team should step in, and the prosecution team should leave the courtroom.

The prosecution and filter teams should prepare together for the hearing. The filter team needs to be in position to handle any aspect of the hearing if the prosecution team needs to leave the courtroom. While the filter team needs to be well-versed in the potentially privileged material, it should also

be prepared to explain in detail how that information fits into the overall fraud if the prosecution team is absent. During that preparation, of course, the filter team should not share any potentially privileged information with the prosecution team.

E. The aftermath

After a court finds that the CFE applies and the communications at issue are not protected by any privilege or protection, the prosecution team can then access the material.

If the material is already in the filter team's possession, the filter team must carefully apply the order to the withheld material. Filter teams often segregate communications from multiple attorneys or about multiple topics. Only the communications at issue in the CFE order can then be provided to the prosecution team.

If the material at issue were subpoenaed, the subpoenaed party must now produce the ordered documents. If testimony were subpoenaed, the witness can be scheduled to appear before the grand jury and respond to questions within the scope of the CFE order.

IV. Benefits of the CFE

A. Obtaining relevant evidence

The main benefit of a successful CFE motion is access to evidence that can further an investigation and provide evidence of fraudulent conduct. At issue in *Zolin*, for example, were privileged communications on audio tapes that were relevant to an Internal Revenue Service criminal investigation into the tax returns of L. Ron Hubbard, the founder of the Church of Scientology.[19.] Other recent cases include obtaining email evidence where a lawyer facilitated a client fraudulently obtaining and expending investment money, including through the use of an Interest on Lawyers' Trust Account (IOLTA),[20.] and obtaining emails and testimony related to a client using his legal representation to defraud plaintiffs in a civil action by lying at his deposition.[21.]

B. Creating a "record of reasonableness"

In our experience, prosecution teams that follow these prophylactic steps while obtaining such evidence create a host of benefits that contribute to the success of their case and enhance the credibility of the prosecutors and agents involved. When prosecution teams obtain court rulings or negotiate with privilege holders before exposure to potentially privileged material, for example, they create a "record of reasonableness" that courts can later look to when allegations are made that the prosecution disregarded privilege, was inadvertently

19. *Zolin*, 491 U.S. at 556.
20. United States v. Liberty, No. 19-cr-30, 2020 U.S. Dist. LEXIS 170941 (D. Me. Feb. 12, 2020).
21. United States v. Hallinan, 290 F. Supp. 3d 355, 367 (E.D. Pa. 2017).

exposed to privileged information, or otherwise made a discovery mistake.

Further, using these steps supports the "document, explain, and defend" philosophy that we described above and will allow the prosecution team later to explain and justify to a presiding judge how carefully it respected privilege while still taking appropriate steps to obtain evidence lawfully.

Separately, advance pretrial findings that the CFE applies will assist with presenting evidence at trial, for example by laying the foundation that certain communications are in furtherance of a conspiracy or are agent statements.

Finally, the prosecution team will benefit from alerting the court to these issues early in an investigation or well before trial, as the court will necessarily review the evidence and form a view of the evidence.

About the Authors

John Kosmidis is the Chief of the Criminal Division, Fraud Section's Special Matters Unit, which handles the Fraud Section's filter matters and litigates privilege issues across the country.

Jerrob Duffy is the Chief of the Criminal Division, Fraud Section's Litigation Unit, which advises the Fraud Section on all litigation matters, including at trial and on appeal.

Page Intentionally Left Blank

The Special Matters Unit: Best Practices for Addressing Attorney–Client Privilege Issues

Lindita V. Ciko Torza
Trial Attorney
Special Matters Unit
Fraud Section

Timothy J. Coley
Assistant Chief
Special Matters Unit
Fraud Section

I. Introduction

White-collar investigations and prosecutions often involve complex and overlapping sets of factors, none of which are made simpler by the privileged material that investigators should not be exposed to. For instance, a typical white-collar case covers a number of corporate targets, subjects, witnesses, and document custodians; potentially multi-jurisdictional and international legal frameworks; sophisticated counsel representing the various parties; potential involvement of the corporate legal function or outside counsel in the fraud; multiple avenues for obtaining documents including search warrants, subpoenas, and voluntary productions; parallel investigations by civil enforcement and regulatory agencies; and multiple defendants entitled to extensive disclosure obligations. Layered on top of these moving parts is an intricate and ever-changing legal landscape regarding how privileged material should be handled.

How can investigators and prosecutors possibly untangle this thicket to avoid serious consequences that may arise when privileged material is not properly handled? The historical solution that investigators have implemented, and that courts have broadly approved, has been to use filter teams—attorneys and support staff separated from the investigators and prosecutors on the matter—to screen out privileged material. As white-collar matters have grown more complex and volumes of evidence have increased, the Fraud Section of the Department of Justice (Department)'s Criminal Division (CRM) decided to establish the Special Matters Unit (SMU)—an independent, specialized,

in-house filter team.[1]

II. The role of filter teams

Filter teams have become necessary in complex white-collar litigation, as courts and defense counsel have become increasingly attuned to potential taint where members of investigation or prosecution teams' access or review potentially privileged material (PPM). Where a prosecutor is deemed to have improperly accessed PPM, defendants are potentially entitled to significant remedies, ranging from evidentiary exclusion to disqualifying the prosecution teams and even dismissing the indictment. Defendants are increasingly launching such attacks. For example, in *United States v. Esformes*, the defendants argued that a prosecutor improperly reviewed privileged material including documents, communications, interviews, and recordings, providing defense strategy to the prosecution.[2] After lengthy hearings and a negative magistrate judge report and recommendation, the district judge suppressed certain portions of evidence, but did not disqualify the prosecution team or dismiss the indictment.[3]

Filter teams are designed to prevent exposure to privileged material, avoiding these problems. In general, filter teams can perform the following functions:

- **Conduct filter searches** on locations that may have potentially privileged data sources, such as an in-house or co located attorney;
- **Conduct document review** and segregation of PPM;
- **Conduct interviews with witnesses**, including lawyers and those who have been given legal advice, who may disclose potentially privileged information;
- **Review covert recordings**, including wiretaps, that may contain potentially privileged communications;
- **Negotiate with defense counsel** on identifying and handling PPM; and
- **Litigate privilege-related issues** in court pre- and post indictment.[4]

The Fraud Section formally created the SMU in 2020 to focus on privilege and legal ethics issues.[5] The unit's role is to preserve defendants' legal

1. U.S. Dep't of Just., Fraud Section Year in Review 4 (2020).
2. No. 16-20549, 2018 WL 5919517, at *12 (S.D. Fla. Nov. 13, 2018).
3. *Id.* at *35; *see also* United States v. Elbaz, 396 F. Supp. 3d 583 (D. Md. 2019); United States v. Stewart, 294 F. Supp. 2d 490 (S.D.N.Y. 2003).
4. *See generally Esformes*, No. 16-20549, 2018 WL 5919517 (discussing role of filter team).
5. Robert A. Zink, Acting Deputy Assistant Att'y Gen., U.S. Dep't of Just., Remarks at Virtual GIR Live Interactive: Regional Spotlight-North America (Dec. 9, 2020). The

privileges and ensure that Fraud Section prosecution teams are not tainted by exposure to privileged information.[6] In addition to the traditional roles of filter teams described above, the SMU also provides training, guidance, and thought leadership on privilege and ethics issues to Fraud Section prosecutors.[7] As described in Part IV, the SMU's privilege review process generally segregates PPM from non-privileged materials in accordance with court-approved protocols,[8] and provides defendants with an opportunity to assert privilege.

III. Types of privilege

Filter teams encounter various and often overlapping privileges and legal protections. The following is a brief overview of the most commonly encountered privileges and protections, as well as recent court guidance on these doctrines' interpretation.

A. Attorney–client privilege

The attorney–client privilege is the oldest of the testimonial privileges that protect confidential communications. The "purpose" of the privilege "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[9] The privilege "protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege."[10] Generally, the attorney–client privilege attaches–

> (1) [w]here legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection be waived.[11]

The attorney–client privilege covers individuals and corporate entities. The latter may assert the attorney–client privilege with respect to its employees'

---

groundwork for the SMU was laid out in mid-2018 with the Privilege Review Team (PRT), a group of attorneys carrying out many of the tasks that the SMU currently undertakes. The PRT was part of the Strategy, Policy, and Training (SPT) section.

6. *Id.*

7. *See* U.S. Dep't of Just., *supra* note 1, at 4.

8. *See e.g.*, *In re* Sealed Search Warrant & Application for a Warrant by Tel. or Other Reliable Elec. Means, 11 F.4th 1235, 1239–42 (11th Cir. 2021), *cert. denied sub nom.* Korf v. United States, No. 21-1364, 2022 WL 4651429 (U.S. Oct. 3, 2022) (describing Attachment B to the search warrant).

9. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

10. Matter of Walsh, 623 F.2d 489, 494 (7th Cir. 1980) (quoting Fisher v. United States, 425 U.S. 391, 403 (1976)).

11. United States v. Ruehle, 583 F.3d 600, 607 (9th Cir. 2009) (quoting *In re* Grand Jury Investigation, 974 F.2d 1068, 1071 n.2 (9th Cir. 1992)); *accord In re* Grand Jury Subpoena Duces Tecum Dated Sept. 15, 1983, 731 F.2d 1032, 1036 (2d Cir. 1984).

confidential communications with its attorneys when (1) the employee seeks legal advice for the entity or provides facts that counsel needs to give the entity legal advice; (2) the employee is aware that the purpose of the communication with counsel is to provide legal advice to the entity; and (3) the communication concerns matters within the scope of the employee's duties.[12.]

The attorney–client privilege "is construed narrowly"[13.] and must be asserted on a "document-by-document basis"; a "blanket claim of privilege that does not specify what information is protected" is insufficient to satisfy a privilege claim.[14.]

B. Joint defense agreements and common interest privilege

The joint defense agreement (JDA) or common-interest privilege (CIP) is not an independent privilege. It is considered an extension of the attorney–client privilege[15.] or "an exception to the general rule that disclosure of documents protected by the work product doctrine or attorney client privilege constitutes a waiver of the protection."[16.]

JDAs are verbal or written agreements between two or more defendants represented by separate attorneys to pool resources. JDAs stipulate that the communications made by any one or more parties to the agreement, to any one or more of the attorneys, shall be deemed a confidential attorney–client communication. Typically, to be protected by a CIP, the law requires that attorneys for the parties be on the communications. A party asserting a joint-defense or common-interest privilege must show that the communication was given in confidence and that the client "*reasonably* understood" it to be so given.[17.] A communication directly among the clients is not privileged unless it was made for the purpose of communicating with a lawyer.[18.] In addition, a party invoking the joint defense privilege must establish that the communication (1) arose "in the course of a joint-defense effort" and (2) was "designed to further that effort."[19.]

---

12. *See Upjohn Co.*, 449 U.S. at 394–95; *In re* Ampicillin Antitrust Litig., 81 F.R.D. 377, 384–86 (D.D.C. 1978).
13. United States v. Naegele, 468 F. Supp. 2d 165, 169 (D.D.C. 2007).
14. United States v. White, 970 F.2d 328, 334 (7th Cir. 1992).
15. Waller v. Fin. Corp. of Am., 828 F.2d 579, 583 n.7 (9th Cir. 1987).
16. Jones v. Tauber & Balser, P.C., 503 B.R. 510, 517 (N.D. Ga. 2013).
17. United States v. Bay State Ambulance & Hosp. Rental Serv., Inc., 874 F.2d 20, 28 (1st Cir. 1989) (citing Kevlik v. Goldstein, 724 F.2d 844, 849 (1st Cir. 1984)); *see also* Matter of Bevill, Bresler & Shulman Asset Mgmt. Corp., 805 F.2d 120, 126 (3d Cir. 1986); United States v. Moss, 9 F.3d 543, 550 (6th Cir. 1993).
18. *See* United States v. Evans, 113 F.3d 1457, 1466–67 (7th Cir. 1997) ("The common interest or joint defense doctrine 'generally allows a defendant to assert the attorney-client privilege to protect his statements made in confidence not to his own lawyer, but to an attorney for a co-defendant for a common purpose related to the defense of both.'" (quoting United States v. Keplinger, 776 F.2d 678, 701 (7th Cir. 1985))).
19. *E.g.*, *In re* Grand Jury Proc. v. United States, 156 F.3d 1038, 1042–43 (10th Cir. 1998).

C. Work product doctrine

The work product doctrine protects from disclosure certain materials that an attorney prepared in anticipation of litigation[20] as well as materials containing an attorney's deliberative process, legal theories, opinions, impressions, or conclusions.[21] Additionally, an attorney's selection of some information from a larger universe of information, such as a compilation of facts, documents, or witnesses, is protected under the work product doctrine when (1) "[t]he compilation reflects the compiler's opinion" and (2) "[t]he requesting party has equal access to the same larger universe of information from which counsel created the compilation."[22]

D. Marital privilege

Courts recognize two types of marital privilege, both of which are testimonial and non-constitutional.[23] The adverse spousal testimony privilege protects one spouse from being compelled to testify against the other. This privilege "allows a spouse called as a witness against his or her [own] spouse in a criminal proceeding to refuse to testify."[24] The other type of spousal communications privilege "protects from disclosure private communications between the spouses in the confidence of the marital relationship."[25] For the privilege to attach, the following prerequisites must be met: "(1) there must have been a communication; (2) there must have been a valid marriage at the time of the communication; (3) the communication must have been made in confidence; and (4) the privilege must not have been waived."[26] Both spouses hold this privilege, which survives divorce.[27]

E. Exceptions to privilege

1. Waiver of the attorney–client privilege

The attorney–client privilege belongs to the client and only the client or client's attorney acting on behalf of the client can waive it.[28] The privilege

20. *See* Fed. R. Crim. P. 16(a)(2), 16(b)(2).
21. *See* Continental Cas. Co. v. Under Armour, Inc., 537 F. Supp. 2d 761, 769 (D. Md. 2008).
22. *Work Product Protection: Overview (Federal)* (Prac. L. Litig. W-025-4967), https://us.practicallaw.thomsonreuters.com/w-025-4967; *see* Sporck v. Peil, 759 F.2d 312, 316 (3d Cir. 1985).
23. Trammel v. United States, 445 U.S. 40, 53 (1980); United States v. Wilson, 505 F. Supp. 3d 3, 12 (D. Mass. 2020) ("Both [spousal testimony and marital communications] privileges are testimonial and not constitutional.").
24. Sec. & Exch. Comm'n v. Lavin, 111 F.3d 921, 925 (D.C. Cir. 1997).
25. *Id.*
26. *Id.* (citations omitted).
27. *Marital Privilege*, Legal Info. Inst., Cornell L. Sch., https://www.law.cornell.edu/wex/marital_privilege (last visited Aug. 11, 2022).
28. *See* United States v. Reyes, 239 F.R.D. 591, 602 (N.D. Cal. 2006) (holding that law firms "surrendered whatever privileges may have attached to the subpoenaed materials when they shared their contents with the government").

is expressly waived when an individual client voluntarily discloses privileged communications—whether intentionally or unintentionally—to third parties outside the attorney–client relationship, or JDA or common interest if applicable.[29] A corporate client may waive privilege through counsel, current management, or employees acting in the corporation's interest.[30] Dissolved corporate entities cannot assert privilege.[31]

A filter team may not be necessary in cases of express, intentional waiver. A filter team, however, is necessary to litigate the other exceptions to privilege.

A client may waive the attorney–client privilege by implication (implied waiver) when it relies on that communication in litigation.[32] Under certain circumstances, courts will interpret the failure to produce a privilege log with sufficient detail to allow a reviewing party or court to assess whether the party's privilege claim is valid.[33]

2. Crime–fraud exception to the attorney–client privilege

Under the crime–fraud exception to the attorney–client privilege, communications that the privilege would otherwise protect are not protected if they further criminal conduct.[34]

3. Joint participation exception to the marital communications privilege

Communications between spouses during a valid marriage are privileged unless they pertain to the commission of a crime in which both spouses are participants.[35]

IV. Filter process

This Part includes a general overview of the SMU's filter process. Note, however, that this process can and should be circuit and district-specific. There is no uniform, nationwide standard for conducting filter reviews, and there is no one size-fits-all protocol that a filter team should follow. Because CRM prosecutes white-collar crime nationwide, the SMU's procedures were crafted with an eye toward being acceptable regardless of the district. They were also designed in response to recent case law regarding filter protocols.

In the search warrant context, the government's process for identifying, segregating, and reviewing PPM is outlined in the "Attachment B" template that the SMU developed for prosecution teams to include in search warrant

29. *See, e.g.*, *In re* Pac. Pictures Corp., 679 F.3d 1121, 1126–27 (9th Cir. 2012).
30. *See* Commodity Futures Trading Comm'n v. Weintraub, 471 U.S. 343, 348 (1985) ("[T]he power to waive the corporate attorney-client privilege rests with the corporation's management and is normally exercised by its officers and directors.").
31. *See, e.g.*, TAS Distrib. Co. v. Cummins Inc., No. 07-1141, 2009 WL 3255297, at *1–2 (C.D. Ill. Oct. 7, 2009).
32. *E.g.*, *In re* County of Erie, 546 F.3d 222, 228 (2d Cir. 2008).
33. *See, e.g.*, Bittaker v. Woodford, 331 F.3d 715, 719–20 (9th Cir. 2003).
34. *In re* Antitrust Grand Jury, 805 F.2d 155, 164 (6th Cir. 1986).
35. *E.g.*, United States v. Broome, 732 F.2d 363, 365 (4th Cir. 1984).

applications where they believe PPM may be present.[36] This Attachment B contains detailed procedures for handling PPM encountered in digital and non-digital evidence. For instance, with respect to digital evidence, the Attachment B provides the following in relevant part:

- The SMU, in consultation with the search team, will compile a list of "privilege search terms" to be used to electronically search the digital devices, including specific names and generic words intended to identify potentially privileged information. The SMU will conduct an electronic review of the data on the digital devices using the privilege search terms, and by using search protocols specifically chosen to identify and segregate documents or data containing potentially privileged information.

- Documents or data that are identified by this review as not potentially privileged, including documents that do not contain the privilege search terms, may be released to the Search Team without court intervention. . . . Documents or data identified during the initial privilege search terms review to be potentially privileged will be segregated. An SMU attorney may thereafter review the segregated documents to confirm whether or not they contain potentially privileged information. If the SMU attorney determines the documents or data are not potentially privileged, they may be given to the Search Team.

- If the SMU attorney determines that documents are potentially privileged, the SMU attorney may do any of the following: (a) apply *ex parte* to the court for a determination whether or not the documents contain privileged information; (b) defer seeking court intervention and instead segregate the documents in a manner that makes them inaccessible to the search team; or (c) disclose the documents to the potential privilege holder, request a privilege log if the potential privilege holder asserts privilege, and seek a ruling from the court regarding the documents if the parties cannot reach agreement.[37]

Courts in numerous circuits, including the Third, Fourth, Fifth, Sixth, and Eleventh Circuits, have expressly approved the use of filter teams and privilege protocols.[38] Some courts, however, have criticized or expressed skepticism regarding certain filter practices. The leading case criticizing filter practices is *In*

36. *See, e.g.*, Partially Opposed Motion for Discovery Protocol Governing Disclosure of Material Subject to Claims of Privilege at 45 (Ex. C), 52 (Ex. D), United States v. Carver, No. 22-cr-80022 (S.D. Fla. Oct. 11, 2022), ECF No. 358 [Attachment B].
37. *Id.* at 48–49.
38. *See* United States v. Salahaldeen, No. 20-cr-839, 2021 WL 2549197 (D.N.J. May 7, 2021); United States v. Reifler, No. 20-cr-512-1, 2021 WL 2253134 (M.D.N.C. June 2, 2021); Order, United States v. Fluitt, No. 20-cr-196 (W.D. La. Dec. 9, 2020), ECF No. 22; Order Granting Motion for Discovery Protocol Governing Disclosure of Material Subject to Claims of Privilege, United States v. Young, No. 19-cr-10040 (W.D. Tenn.

re Search Warrant, also known as *Baltimore Law Firm*.[39] In this case, the government seized documents pursuant to a search warrant for a lawyer's records, including communications with the lawyer's other clients that were being investigated or prosecuted by the same United States Attorney's Office for unrelated crimes.[40] The Fourth Circuit criticized that filter team's practices, particularly because it failed to provide the target law firm with an adversarial opportunity to contest the process, delegated privilege determinations to non-attorney filter team members, and failed to consider the privilege interests of the law firm's other clients whose documents were contained within the search warrant returns.[41] As a result, the Fourth Circuit concluded that the filter process in that case "improperly delegated judicial functions to the Filter Team. And the magistrate judge failed to recognize and consider the significant problems with that delegation, which left the government's fox in charge of guarding the Law Firm's henhouse."[42]

In part due to the guidance offered in *Baltimore Law Firm* and other subsequent cases,[43] the SMU adapted its filter review process to provide notice and opportunity for input from ostensible privilege holders wherever practicable and for obtaining court-approved or agreed-upon protocols in many cases. The search warrant Attachment B and the privilege protocol provisions described above likewise were created to address the concerns raised in *Baltimore Law Firm* and other decisions. They delineate a clear privilege assertion process supported by objective application of keyword search terms, as well as a detailed mechanism for resolving any privilege disputes through the courts. Courts have approved this process even over vociferous objection from defense counsel who have argued, amongst other things, that no government attor-

---

Oct. 15, 2020), ECF No. 182; *In re* Sealed Search Warrant & Application for a Warrant by Tel. or Other Reliable Elec. Means, 11 F.4th 1235, 1239 (11th Cir. 2021) (*Korf*).

39. *In re* Search Warrant Issued June 13, 2019 (*Baltimore Law Firm*), 942 F.3d 159 (4th Cir. 2019).

40. *Id.* at 166–67.

41. *Id.* at 177–80. The court summarized that, "[i]n approving the Filter Team and its Protocol, the magistrate judge made several legal errors by, inter alia: (1) assigning judicial functions to the Filter Team; (2) authorizing the Filter Team and its Protocol in *ex parte* proceedings that were conducted prior to the search and seizures at the Law Firm; and (3) failing to properly weigh the foundational principles that protect attorney-client relationships." *Id.* at 176.

42. *Id.* at 178.

43. Other significant cases critical in some respects to filter teams include *In re* Grand Jury Subpoenas 04-124-03 and 04-124-05 (*Winget*), 454 F.3d 511 (6th Cir. 2006) and *Korf*, 11 F.4th 1235. Nevertheless, both *Winget* and *Korf* expressly recognize the propriety and utility of filter teams. *Winget*, 454 F.3d at 522–23 (noting that using a filter team to make initial privilege determinations is "respectful of, rather than injurious to, the protection of privilege"); *Korf*, 11 F.4th at 1249–50 ("Second, the Intervenors cite no cases for the broad remedy they seek: a holding that government agents 'should never . . . review documents that are designated by their possessors as attorney-client or work product privileged' until after a court has ruled on the privilege assertion.' Nor has our research unearthed any." (emphasis omitted)).

ney—including segregated members of the filter team—should have access to their clients' PPM.[44]

Indeed, recent high-profile criminal investigations and prosecutions, including those of attorneys Michael Avenatti and Rudolph Giuliani, have yielded favorable language regarding filter teams. In *United States v. Avenatti*, the U.S. District Court for the Southern District of New York explained that filter teams generally may access and review material for privilege: "[S]o long as the putative privilege holder . . . has notice and the opportunity to raise objections with the court before [PPM] are disclosed to members of the prosecution team, it offends neither the law of privilege nor the Fourth Amendment to allow the Government to make the first pass."[45] The *Giuliani* court also rejected a similar argument that ostensible privilege holders should obtain a "first cut" review of privileged materials obtained via search warrant before the filter team may access them:

> Giuliani and Toensing argue that the materials seized pursuant to the April 2021 warrants should be returned to them so that they may review them in the first instance for responsiveness and privilege. . . . There is no legal requirement for the Government to proceed by subpoena, nor is there any basis for the subject of an investigation to require it to do so.[46]

Accordingly, although defendants—and certain courts—remain skeptical of filter teams' ability to obtain and review PPM, the landscape post-*Baltimore Law Firm* largely supports their role so long as filter teams remain cognizant of the state of the law and proactively model their processes to reflect court guidance and anticipate future challenges.

V. Meeting the government's disclosure obligations

The government's disclosure obligations under *Brady*, *Giglio*, the Jencks Act, and Rule 16 require production of material to criminal defendants.[47] Complexities arise, however, when privilege protects the material potentially subject to disclosure.[48] As a result, the SMU will often seek court-approved or privilege holder-agreed protocols governing the handling of PPM. These court-approved privilege protocols generally set forth a similar process as described in Attachment B above, including:

- Material not identified as containing PPM following the filter team's

44. *See, e.g.*, Order on Gov't's Motion for Discovery Protocol, United States v. Stein, No. 21-cr-20321 (S.D. Fla. Oct. 29, 2021), ECF No. 58; United States v. Carver, No. 22-80022-cr, 2022 WL 1681917 (S.D. Fla. May 9, 2022).
45. 559 F. Supp. 3d 274, 284 (S.D.N.Y. 2021).
46. *In re* Search Warrants Executed on Apr. 28, 2021, No. 21-MC-425, 2021 WL 2188150, at *1 (S.D.N.Y. May 28, 2021).
47. Justice Manual 9-5.002.
48. *See* Swidler & Berlin v. United States, 524 U.S. 399, 403 (1998); United States v. W.R. Grace, 439 F. Supp. 2d 1125, 1142–45 (D. Mont. 2006).

application of objective keyword search terms, including after receiving input from the ostensible holder of the potential privilege(s) or protection(s) regarding those terms, where identifiable, and the filter team's privilege review, may be produced to the prosecution team and defendant(s) without the need for the court's approval.

- Before producing PPM to prosecution team, the filter team will provide written notice to ostensible holders of the potential privilege(s) or protection(s) and provide a timeframe for the claimant(s)' written objection in the form of a privilege log specifically asserting the privilege or protection on a document by document basis.

- If the ostensible holder of the potential privilege(s) or protection(s) fails to object within the specified period, the filter team will provide the prosecution team and defendant(s) with information regarding the filter team's attempts to contact the ostensible holder and move the court for a finding that the ostensible holder of the potential privilege(s) or protection(s) has waived any privilege(s), protection(s), or both over the PPM.

- If the filter team and ostensible holder of the potential privilege(s) or protection(s) disagree regarding any privilege assertions, they will meet and confer to try and resolve any disagreements concerning the objection(s), with notice to any co defendants who may wish to attend. If no resolution is achieved, the filter team, co-defendant(s), or both will move to compel production of the disputed PPM within the specified timeframe. Timeframes for opposition and reply briefs are likewise specified within the protocol.

- The SMU's privilege protocols also contain protections under Federal Rule of Evidence 502(d), providing that any PPM that is produced to the prosecution team, defendant(s), or a non-party under this protocol or subsequent order in this proceeding, shall not constitute a waiver or forfeiture of any privilege or protection claim in any other federal or state judicial or administrative proceeding.

- The privilege protocols also provide that if any prosecution team member inadvertently reviews PPM, the prosecution team member shall immediately cease review of the PPM and turn the PPM over to the filter team for processing in accordance with this protocol. Inadvertent review of PPM shall not automatically disqualify a prosecution team member from this matter.[49.]

The goal of these protocols is to have court supervision of a process where privilege holders, including non-parties, are required to log their assertions and

49. *See* Attachment B, *supra* note 36.

where all parties must litigate privilege issues on a set timeframe. The protocols also require court approval of a process that balances disclosure obligations and privilege holders' rights so that the government cannot be accused of withholding material subject to its obligations. To date, the SMU has obtained numerous protocol orders across the country.[50]

VI. Challenges looking forward

Filter teams face immense challenges due to the sheer volume of content stored in seized hard drives, laptops, tablets, and phones. When the government seizes a target's computers or hard drives, it takes custody of thousands, if not millions, of documents and metadata. For example, Apple's iCloud, which is available to all individual iPhone users, provides 5 gigabytes (GB) of free storage.[51] One GB is equivalent to approximately 65,000 pages of Microsoft Word files and approximately 678,000 pages of text files.[52] An organization produces and stores exponentially more data.[53] Reviewing these files in a timely manner is a challenge to both filter teams and, subsequently, prosecutors. Further, defendants or potential targets are sometimes not aware of all privileged materials seized.

Significant challenges are also posed by using sophisticated encryption tech-

---

50. *See, e.g.*, Order, United States v. Trotta, No. 21-cr-60260 (S.D. Fla. Jan. 18, 2022), ECF No. 37; United States v. Murillo Prijic, No. 21-cr-60340, 2021 WL 6111657 (S.D. Fla. Dec. 27, 2021); Order, United States v. Port, No. 19-cr-20583 (S.D. Fla. Nov. 30, 2021), ECF No. 194; United States v. Letko, No. 19-20652, 2021 WL 3674116 (E.D. Mich. Aug. 10, 2021); United States v. Stein, No. 21 20321, 2021 WL 3781926 (S.D. Fla. Aug. 25, 2021); Order, United States v. Murphy, No. 20-cr-291 (N.D. Ala. July 26, 2021), ECF No. 74; United States v. Siefert, No. 21-2, 2021 WL 3076940 (E.D. Ky. July 19, 2021); United States v. Swiencinski, No. 18-cr-368, 2021 WL 2701265 (S.D. Tex. May 3, 2021); Order, United States v. Kennedy, No. 19-cr-842 (S.D. Tex. Apr. 21, 2021), ECF No. 32; Order, United States v. Garipoli, No. 19-cr-80196 (S.D. Fla. Mar. 11, 2021), ECF No. 60; Order, United States v. Comu, No. 19-cr-112 (N.D. Tex. Jan. 8, 2021), ECF No. 314; Order, United States v. Fluitt, No. 20-cr-196 (S.D. Fla. Dec. 9, 2020), ECF No. 22; United States v. Satary, 504 F. Supp. 3d 544 (E.D. La. 2020); Order, United States v. Canchola, No. 19-cr-473 (N.D. Tex. Nov. 25, 2020), ECF No. 65; Order Granting Motion for Discovery Protocol Governing Disclosure of Material Subject to Claims of Privilege, United States v. Young, No. 19-cr-10040 (W.D. Tenn. Oct. 15, 2020), ECF No. 182; Order, United States v. Hanley, No. 19-cr-120 (M.D. La. July 16, 2020), ECF No. 65; United States v. Patel, No. 19-cr-80181, 2020 WL 3118291 (S.D. Fla. June 8, 2020).

51. *iCloud+ Plans and Pricing*, Apple (June 17, 2022), https://support.apple.com/en-us/HT201238.

52. LexisNexis, How Many Pages in a Gigabyte 1, https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf.

53. *See, e.g.*, Joe Dysart, Ditching Dark Data: Set a Schedule to Dump Useless Info, A.B.A. J., Apr. 2013, at 32 ("[T]he metric used to gauge the size of corporate databases these days is now expressed in petabytes. A single petabyte . . . [stores the equivalent of] about 20 million four-drawer file cabinets filled with text.").

nologies that may impair proper extraction of data from phones. Ever-changing communication applications and enhanced privacy features complicate filter teams' work because they make it more difficult to identify potentially privileged information and the custodians of such information.

These challenges are not necessarily unique to filter matters. Challenges continue to be felt acutely due to the dynamic legal landscape facing filter issues, filter teams generally being under a microscope, voluminous and encrypted data, and related resource constraints.

VII. Alternatives to filter reviews

Considering these challenges and defendants' increasing propensity for contesting filter issues, prosecuting units may want to consider the alternatives to a filter team-staffed filter review, depending on the matter.

- **Seek entry of an order under Federal Rule of Evidence 502(d) with privilege holders' agreement**. Rule 502(d) states: "A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding."[54] In other words, the parties may agree to release PPM to the prosecution team and effectively defer resolution of any privilege issues as an evidentiary matter if necessary.

- **Obtain an express waiver**. If the privilege holder wishes to waive their privileges and protections, they may provide an express written waiver. Note, however, that Department policy restricts the government's ability to request waivers from corporations.[55] Accordingly, the privilege holder itself generally must initiate express waivers.

- **Seek appointment of a special master**. Special masters are independent, court-appointed individuals who perform many of the same functions as filter teams. They are most utilized in complex cases and typically are very costly. Former Fraud Section Chief Robert Zink, who oversaw the creation of the SMU, estimated that appointing a special master to each white-collar case in place of the SMU would cost the Department approximately $2–3 million per matter.[56]

- **Issue a document subpoena in lieu of a search warrant**. In many instances, issuing a subpoena for material likely containing PPM may not require a back-end filter review because the recipient will have the opportunity to review the material for privilege prior to production, unlike a search warrant.

54. Fed. R. Evid. 502(d).
55. Justice Manual 9-28.710.
56. Adam Dobrik, *Rob Zink: Special Masters Would Solve DOJ Privilege Concerns*, Glob. Investigations Rev. (Oct. 28, 2021).

- **Narrow collection efforts to prevent a need for filter in the first place**. Perhaps the easiest way to avoid involving filter teams and large-scale filter reviews is to avoid collecting PPM to the greatest extent possible. Where a document custodian is known to possess PPM or otherwise be represented, discuss with your investigation and prosecution team whether that material is necessary before applying for a search warrant. The tendency to over-collect can create a number of discovery related issues in prosecutions, including unnecessary, time consuming filter reviews.

VIII. Conclusion—best practices

Considering the constantly changing landscape facing privilege issues and filter reviews, the best practice for prosecutions teams—if they encounter or reasonably expect to encounter PPM in their investigations or prosecutions—is to confer with the SMU or affiliated filter team as early as possible.

Pre-Indictment

In the pre-indictment context, prosecution teams should ensure that the search warrant Attachment B is included in search warrant applications if it is expected that PPM will be captured. Where executing premises searches, it is recommended to have a filter agent assigned and have a filter attorney available—either physically or virtually—to answer any questions regarding handling PPM during the search. In addition, where appropriate, prosecutors may wish to request the grand jury court for entry of a privilege protocol to get a preemptive court sign-off on the filter process, on top of the process set forth in the search warrant Attachment B.

As noted above, the simplest advice to minimize the likelihood of unnecessary privilege disputes is to be intentional about the material collected and, where possible and appropriate, to avoid collecting material known to contain PPM. Remember that not everything needs to go through filter; only seized materials where PPM is reasonably expected to be found.

Post-Indictment

Following indictment, as soon as practicable, prosecutors should seek entry of the standard privilege protocol (or re entry, if a pre indictment protocol were entered). If there are certain sets of documents that are higher priority from a case strategic standpoint, the filter team should be advised to determine whether rolling reviews and productions are possible. This arrangement enables the prosecution team to obtain the most important documents first while the remaining documents are undergoing the full-scale filter review.

Finally, as with any filter matter, it is important that the prosecution team maximize communication with the filter team and keep them apprised of upcoming deadlines such as trial extensions, discovery deadlines, or pretrial motions deadlines; changes in case status; or any privilege issues that the court or defense flagged.

About the Authors

Lindita V. Ciko Torza serves as Trial Attorney with the Special Matters Unit. Before joining the SMU, she worked as an Associate Attorney in the New York office of a national law firm, advising clients on anti-corruption compliance, international trade law, and international arbitration.

Timothy J. Coley serves as Assistant Chief of the Special Matters Unit. Before joining the SMU, he was counsel in the Washington, D.C., office of a national law firm, practicing in the areas of white-collar, government enforcement, and complex commercial litigation.

Prosecutions in the Securities and Commodities Markets

Justin Weitz
Former Acting Principal Deputy Chief
Market Integrity and Major Frauds Unit
Fraud Section
Criminal Division

Jennifer Farer
Trial Attorney
Market Integrity and Major Frauds Unit
Fraud Section
Criminal Division

I. Introduction[1]

The federal securities and commodities laws establish a range of obligations for participants in the securities and commodities markets. Violations of many of these provisions can lead to criminal prosecutions, civil enforcement actions brought either independently or in parallel with a criminal prosecution, and civil actions brought by private parties.

In this article, we summarize the options available to federal prosecutors seeking to bring criminal cases involving securities and commodities fraud and market manipulation. We also discuss general securities and commodities fraud statutes and certain implementing regulations thereunder, as well as statutory provisions applicable to specific types of misconduct involving securities and commodities. Finally, we provide examples from recent prosecutions to illustrate the development of cases and legal theories under these provisions. Notably, while this article focuses on criminal prosecutions, civil enforcement actions and private litigation have heavily influenced the body of applicable case law.

II. General securities and commodities fraud statutes

A. Securities Act of 1933 and Securities Exchange Act of 1934

In the wake of the 1929 stock market crash that precipitated the Great Depression, Congress passed the Securities Act of 1933 ('33 Act or Securities

1. The authors are grateful to Vijay Shanker, Deputy Chief, Criminal Division, Appellate Section, for his assistance with research contained within this article.

Act)[2] and the Securities Exchange Act of 1934 ('34 Act or Exchange Act)[3] to protect investors and establish a securities enforcement regime grounded in disclosure and transparency. The '33 and '34 Acts, which were subsequently amended, contain multiple provisions for which willful misconduct constitutes criminal activity.

The '33 and '34 Acts require securities issuers and promoters to provide full and truthful information to investors and the market. These statutes employ extraordinarily broad definitions of what constitutes a security.[4] Beyond the disclosure and registration requirements that form the core of securities regulation in the United States, the '33 and '34 Acts contain general anti-fraud provisions.

The '33 Act's anti-fraud provision, section 17(a), is titled "[u]se of interstate commerce for purpose of fraud or deceit[.]" The statute provides the following:

> It shall be unlawful for any person in the offer or sale of any securities (including security-based swaps) or any security-based swap agreement . . . by the use of any means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly—
>
> > (1) to employ any device, scheme, or artifice to defraud, or
> >
> > (2) to obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or
> >
> > (3) to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.[5]

Section 10(b) of the '34 Act makes it illegal—

> To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement[,] any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.[6]

---

2. Pub. L. No. 73-22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. §§ 77(a), *et seq.*).
3. Pub. L. No. 73-290, 48 Stat. 881 (1934) (codified as amended at 15 U.S.C §§ 78(a), *et seq.*).
4. *See* 15 U.S.C. §§ 77b(a)(1), 78c(a)(10) (defining "security" for each statutory scheme).
5. 15 U.S.C. § 77q.
6. 15 U.S.C. § 78j(b).

Section 10(b) is generally read in conjunction with the U.S. Securities and Exchange Commission's (SEC) implementing regulation, Rule 10b-5,[7] which incorporates anti-fraud language substantially similar to the '33 Act's general anti-fraud provision.

For criminal liability to attach under either statute, there must be a showing of willfulness. Upon such a showing, the statutory maximum penalty for a violation of the '33 Act is 5 years' imprisonment and a $10,000 fine,[8] while the statutory maximum penalty for an individual's '34 Act violation is 20 years' imprisonment and a $5 million fine.[9]

Courts have interpreted these provisions—especially section 10(b) of the '34 Act and Rule 10b-5—to encompass all types of securities fraud. The Supreme Court has described Rule 10b-5 as "broad" and "inclusive," and observed that "Congress intended securities legislation enacted for the purpose of avoiding frauds to be construed 'not technically and restrictively, but flexibly to effectuate its remedial purposes.'"[10] This broad interpretation has allowed prosecutors and regulators to utilize "Rule 10b-5 to reach a wide range of deceitful securities trading practices," including those that might not fall within traditional definitions of securities fraud.[11]

B. Commodity Exchange Act (CEA)

The CEA expressly prohibits manipulation and fraud in multiple sections and authorizes both civil and criminal enforcement and penalties.[12]

First, section 9(a)(2) of the CEA makes it a felony to engage in various forms of manipulative or fraudulent conduct, which is punishable by a maximum fine of $1 million, 10 years' imprisonment, or both.[13] This conduct includes manipulation, attempted manipulation, or swapping the price of any commodity in interstate commerce, any commodity for future delivery (commonly called a "futures contract") that is traded on registered exchanges, or to engage in various forms of false statements or reporting.[14]

Second, in the wake of the financial crisis of 2008, with the Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd–Frank),[15] Congress amended section 6(c) of the CEA to expand and strengthen the statute's anti-fraud and manipulation provisions. As part of the amendments, Dodd–Frank

---

7. 17 C.F.R. § 240-10b-5.
8. 15 U.S.C. § 77x.
9. 15 U.S.C. § 78ff(a). Courts have generally held that, should an alternative fine under 18 U.S.C. § 3571(d) apply, such a fine can exceed the statutory maximum in the '33 or '34 Acts.
10. Affiliated Ute Citizens of Utah v. United States, 406 U.S. 128, 151 (1972) (quoting SEC v. Cap. Gains Rsch. Bureau, Inc., 375 U.S. 180, 195 (1963)).
11. United States v. Charnay, 537 F.2d 341, 348 (9th Cir. 1976).
12. Pub. L. No. 74-675, 49 Stat. 1491 (1936) (codified as amended at 7 U.S.C. §§ 1, *et seq.*).
13. 7 U.S.C. § 9(a)(2).
14. 7 U.S.C. § 13(a).
15. Pub. L. No. 111-203, 124 Stat. 1376 (2010).

added, inter alia, new anti-fraud and manipulation provisions that prohibited using or employing any manipulative or deceptive device and made it unlawful to manipulate or attempt to manipulate the price of any swap or commodity.[16] Under these provisions, it is—

> unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate by not later than 1 year after July 21, 2010, provided no rule or regulation promulgated by the Commission shall require any person to disclose to another person nonpublic information that may be material to the market price, rate, or level of the commodity transaction, except as necessary to make any statement made to the other person in or in connection with the transaction not misleading in any material respect.[17]

In addition, it is "unlawful for any person, directly or indirectly, to manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity."[18] Dodd–Frank also expanded the CEA's existing prohibition against false statements made in registration applications or reports filed with the Commodity Futures Trading Commission (CFTC) to prohibit making any false or misleading statement of material fact to the CFTC in any context.[19]

The CFTC promulgated Rules 180.1 and 180.2 to implement the provisions of the CEA that prohibit the employment, or attempted employment, of manipulative or deceptive conduct and manipulation of pricing. Promulgated pursuant to section 6(c)(1), Rule 180.1(a): "Prohibition on the employment,

16. The amendments did not replace but rather added to the existing CEA anti-fraud and manipulation provisions. The CEA and regulations thereunder specified that the amendments do not affect the applicability of CEA section 9(a)(2). *See* 7 U.S.C. § 9(1)(B). In addition, in promulgating the final rule under section 6(c)(1), the CFTC explained that CEA section 6(c)(1) and final Rule 180.1 do not affect the applicability of CEA section 4b and "augment the Commission's existing authority to prohibit fraud and manipulation." Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,401 (July 14, 2011). As a result, there are multiple provisions under which prosecutions may be brought for market manipulation and other fraudulent activity.

17. 7 U.S.C. § 9(1). This section also included a "Special provision for manipulation by false reporting," stating that unlawful manipulation includes delivering a false or misleading or inaccurate report concerning crop or market information or conditions that affect or tend to affect the price of any commodity in interstate commerce, but also providing for a "Good faith mistakes" exception. 7 U.S.C. § 9(1)(A), (C).

18. 7 U.S.C. § 9(3).

19. 7 U.S.C. § 9(2).

or attempted employment, of manipulative and deceptive devices" provides in relevant part—

> It shall be unlawful for any person, directly or indirectly, in connection with any swap, or contract of sale of any commodity in interstate commerce, or contract for future delivery on or subject to the rules of any registered entity, to intentionally or recklessly:
>
> > (1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
> > (2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;
> > (3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person; or,
> > (4) Deliver or cause to be delivered, or attempt to deliver or cause to be delivered, for transmission through the mails or interstate commerce, by any means of communication whatsoever, a false or misleading or inaccurate report concerning crop or market information or conditions that affect or tend to affect the price of any commodity in interstate commerce, knowing, or acting in reckless disregard of the fact that such report is false, misleading or inaccurate. Notwithstanding the foregoing, no violation of this subsection shall exist where the person mistakenly transmits, in good faith, false or misleading or inaccurate information to a price reporting service.[20.]

Rule 180.2: "Prohibition on price manipulation," promulgated pursuant to section 6(c)(3) and the CFTC's general rulemaking authority, mirrors the statutory text and provides as follows: "It shall be unlawful for any person, directly or indirectly, to manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity."[21.]

Importantly, section 6(c)(1) of the CEA and Rule 180.1 are modeled on section 10(b) of the Exchange Act[22.] and the SEC's Rule 10b-5.[23.] In promulgating the rule, the CFTC acknowledged the virtually identical statutory language and stated the following:

> To account for the differences between the securities markets and the derivatives markets, the Commission will be guided, but not

20. 17 C.F.R. § 180.1.
21. 17 C.F.R. § 180.2.
22. 15 U.S.C. § 78j(b).
23. 17 C.F.R. § 240-10b-5.

> controlled, by the substantial body of judicial precedent applying the comparable language of SEC Rule 10b-5. Such extensive judicial review serves as an important benefit to the Commission and provides the public with increased certainty because the terms of Exchange Act Section 10(b) and SEC Rule 10b-5 have withstood challenges to their constitutionality in both civil and criminal matters.[24]

As with the SEC's Rule 10b-5, Rule 180.1 is intended to be flexible to effectuate its purpose, and a violation of Rule 180.1 does not require proof of a market or price effect.

Thus, while there are a variety of differences between the CEA and securities laws, driven in part by the differences in the markets and products they respectively regulate, courts addressing violations of the CEA and the CFTC's regulations thereunder have relied heavily on the body of legal precedent interpreting the securities laws. As with the securities statutes discussed above, the CEA imposes criminal penalties for willful violations of the CEA or the CFTC's rules and regulations thereunder.[25]

C. 18 U.S.C. § 1348

Congress originally enacted section 1348 in 2002 as part of the Sarbanes–Oxley Act and subsequently amended it in 2009 to include commodities involving options or futures contracts. It is generally a straightforward criminal statute, closely analogous to the bank, mail, and wire fraud statutes, with two subsections that offer different methods of establishing criminal liability for securities and commodities fraud. Specifically, the statute provides the following:

> Whoever knowingly executes, or attempts to execute, a scheme or artifice—
>
> > (1) to defraud any person in connection with any commodity for future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78*l*) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78*o*(d)); or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any commodity for

24. Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,398-01, 41,399 (July 14, 2011).

25. 7 U.S.C. § 13(a)(5). This section also provides, however, that "no person shall be subject to imprisonment under this paragraph for the violation of any rule or regulation if such person proves that he had no knowledge of such rule or regulation." *Id.*

> future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78*l*) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78*o*(d));
>
> shall be fined under this title, or imprisoned not more than 25 years, or both.[26.]

Importantly, section 1348 is generally understood to require a showing of an intent to defraud.[27.] A conspiracy to violate section 1348 may be charged under 18 U.S.C. § 1349, with no overt act requirement.[28.]

Found in the federal criminal code, section 1348 lacks a civil parallel and therefore cannot be used by the SEC, CFTC, other civil enforcement authorities, or private plaintiffs. Criminal prosecutors can utilize section 1348 to combat various types of securities and commodities fraud, including, but not limited to, insider trading, accounting fraud, and various forms of market manipulation. Notably, there is a six-year statute of limitations for certain securities fraud offenses, including section 1348.[29.] Charging under this provision provides for an additional year as compared to the five-year limitations period applicable to the CEA and other general fraud provisions, such as wire and mail fraud.

III. Specific violations of the securities and commodities laws

A. Market manipulation

While market manipulation cases can often be prosecuted using the general anti-fraud provisions discussed above, there are also statutory provisions that proscribe specific types of manipulative trading activity that can be used for a criminal prosecution.

Both the Exchange Act and the CEA prohibit market manipulation, but Congress did not define the term in either act. The Supreme Court has explained that securities manipulation "connotes intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities."[30.] This conduct can take several forms, including open market manipulation as well as specific types of activity, "such as wash sales,

26. 18 U.S.C. § 1348. See Sandra Moser & Justin Weitz, *18 U.S.C. 1348—A Workhorse Statute for Prosecutors*, 66 DOJ J. Fed. L. & Prac., no. 5, 2018, at 111, for a more extensive discussion of section 1348.
27. *See* United States v. Coscia, 866 F.3d 782, 796 (7th Cir. 2017) (citing United States v. Mahaffy, 693 F.3d 113, 125 (2d Cir. 2012)).
28. *See* United States v. Roy, 783 F.3d 418, 420 (2d Cir. 2015) (citing cases).
29. 18 U.S.C. § 3301.
30. Ernst & Ernst v. Hochfelder, 425 U.S. 185, 199 (1976).

matched orders, or rigged prices, that are intended to mislead investors by artificially affecting market activity."[31] The courts have applied this precedent in evaluating the application of the commodities laws to various forms of market manipulation.[32] As discussed in examples below, many forms of specific manipulative conduct are expressly prohibited by statute.[33]

Because prosecutions under the specific market manipulation provisions of the Securities Act, Exchange Act, and CEA can take many forms, and there may be few cases that courts can look to that address the specific type of fraudulent activity at issue, prosecutors are advised to consider pursuing market manipulation cases under the general anti-fraud provisions of these statutes or other more common types of fraud. Such an approach has several advantages. First, case law in every circuit supports broad interpretations of these statutes. Second, pattern jury instructions for securities fraud exist in multiple circuits. They do not exist for most of the specific types of manipulative conduct discussed below. These pattern jury instructions can serve as a guide for an instruction on commodities fraud, to the extent there is not a pattern instruction for commodities fraud in a particular circuit. Third, grounding market manipulation cases in statutory fraud language often provides a more compelling narrative and allows prosecutors to present evidence of a scheme, as opposed to what may otherwise be perceived as technical violations. Rather than situate market manipulation as its own type of misconduct, prosecutors are advised to rely on the clear precedent that market manipulation is a form of fraud on the market.[34]

Alternatively, or in addition, prosecutors can pursue a manipulation case under a statutory provision that specifically proscribes the conduct at issue. For example, section 9(a) of the '34 Act describes multiple types of manipulative market activity, which, if performed willfully, constitute independent violations of the securities laws and carry the same penalties as violations of section 10(b).[35] Similarly, the CEA contains a "[p]rohibited transactions" provision that identifies various types of prohibited trading activity, which, when undertaken with the requisite knowledge and intent, can also carry criminal penalties.[36] While these statutes explicitly prohibit the identified type of ma-

31. Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 476 (1977).
32. *See, e.g.*, *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 529 n.96 (S.D.N.Y. 2008) (noting that the Court in *Hochfelder*, 425 U.S. at 193–94, was discussing securities fraud but that "its language is equally applicable to commodities fraud").
33. In contrast, open market manipulation does not involve trading activity that is expressly prohibited; instead, the trading at issue seems legitimate on its face. Accordingly, criminal prosecutions and civil enforcement actions addressing this type of fraud are usually brought under the general anti-fraud and anti-manipulation provisions discussed above.
34. *See, e.g.*, United States v. Chanu, 40 F.4th 528, 542 (7th Cir. 2022) (endorsing use of "spoofing" theory in wire fraud case).
35. 15 U.S.C. § 78i(a).
36. 7 U.S.C. § 6c.

nipulative behavior, the body of case law interpreting these provisions is more limited, particularly in the criminal context. This is often because prosecutors and the civil regulators have preferred to pursue spoofing, match or wash trading, and other types of manipulation cases using the general anti-fraud provisions. Because the unit of prosecution for at least some of these specific statutory violations appears to be pegged to specific trades or orders as opposed to scheme liability, it can be easier to demonstrate the requisite criminal intent by charging manipulation cases as schemes to defraud under the general anti-fraud provisions. It is important to be aware of these options when making charging decisions.

Prosecutors may elect to pursue multiple theories simultaneously by charging broader scheme-based statutes alongside more specific statutes. For instance, in a spoofing case where the conduct spans a multi-year period, a prosecutor might charge a single count of commodities fraud under section 1348 to cover the entire scheme alongside multiple spoofing counts pegged to specific illegal transactions. This approach has been used successfully in various prosecutions in recent years and can provide juries with multiple paths to conviction.

While there are many types of manipulation, we choose to highlight two common forms of manipulative trading that the '34 Act and the CEA explicitly prohibit.

1. Spoofing

"Spoofing is a disruptive trading practice in which a person submits bids or offers with the intent to cancel the bid or offer before it is executed."[37] These bids (that is, buy orders) or offers (that is, sell orders), which are quickly canceled, falsely signal to the market that supply or demand for the traded product is greater than it actually is.

The CEA expressly criminalizes spoofing by making it unlawful to "engage in any trading, practice, or conduct on or subject to the rules of a registered entity that . . . is, is of the character of, or is commonly known to the trade as 'spoofing' (bidding or offering with the intent to cancel the bid or offer before execution)."[38] In recent years, the Department of Justice (Department) has focused substantial attention on pursuing spoofing in commodities futures markets.[39]

The '34 Act criminalizes spoofing as well, although not by name. Section 9(a)(2) of the '34 Act makes it unlawful "[t]o effect, alone or with one or more other persons, a series of transactions in any security . . . creating actual or apparent active trading in such security or raising or depressing the price of such security . . . , for the purpose of inducing the purchase or sale of such

37. United States v. Coscia, 4 F.4th 454, 459 n.1 (7th Cir. 2021).
38. 7 U.S.C. § 6c(a)(5)(C); *see also* 7 U.S.C. § 13(a)(2).
39. *See, e.g.*, United States v. Smith, No. 19-cr-669 (N.D. Ill.); United States v. Vorley, No. 18-cr-35 (N.D. Ill.); United States v. Coscia, 866 F.3d 782, 786 (7th Cir. 2017).

security by others."[40] This provision is intended to "outlaw every device 'used to persuade the public that activity in a security is the reflection of a genuine demand instead of a mirage.'"[41] Canceled orders, which have the effect of creating apparent active trading, can thus be prosecuted under the '34 Act.

2. Wash and match trading

Wash trading refers to traders who trade with themselves, often using pseudonymous or nominee accounts. There is no change in beneficial ownership of the security or commodity. Match trading refers to trading by individuals who trade with a prearranged counterparty. These prearranged orders match on an exchange, thus broadcasting a false signal of a bona fide transaction. Wash and match trading can be manipulative, especially in lightly traded securities and commodities, because they may suggest to the public that there is more demand and trading volume than actually exists.

Section 9(a)(1)(A) of the '34 Act prohibits wash trades, that is, "any transaction . . . which involves no change in the beneficial ownership thereof," "for the purpose of creating a false or misleading appearance of active trading . . . ."[42] Section 9(a)(1)(B)-(C) prohibits match trading.

Under the CEA, section 4c(a)(2) prohibits any "transaction that—(A) (i) is, of the character of, or is commonly known to the trade as, a 'wash sale' or 'accommodation trade'; or (ii) is a fictitious sale; or (B) is used to cause any price to be reported, registered, or recorded that is not a true and bona fide price."[43]

B. Accounting fraud under the securities laws

One of the most prominent white-collar criminal investigations of the 21st century involved the collapse of Enron, the Texas based energy services company that disintegrated in the wake of massive accounting fraud allegations. The Enron scandal contributed to the demise of Arthur Andersen, formerly one of the world's largest accounting firms, and prompted the passage of the Sarbanes–Oxley Act of 2002.

Since before Enron, prosecutors and law enforcement agencies have doggedly pursued accounting fraud cases involving publicly traded companies. These investigations focus on one of the most challenging subsets of white-collar crime. They often involve complex accounting across multiple years and business segments and can reflect a corporate culture that diffuses responsibility among culpable actors. While accounting improprieties are usually charged as securities fraud under the general anti-fraud statutes, three additional statutory provisions can assist prosecutors in accounting fraud investigations.

Publicly traded companies, often referred to as issuers, have various reporting and compliance obligations. These obligations often create responsibility

40. Crane Co. v. Westinghouse Air Brake Co., 419 F.2d 787, 794 (2d Cir. 1969).
41. *Id.* (quoting 3 Louis Loss, Securities Regulation 1549–55 (2d ed. 1961)).
42. 15 U.S.C. § 78i(a)(1)(A).
43. 7 U.S.C. § 6c(a)(2).

for senior corporate officers, such as the chief executive officer (CEO) and chief financial officer (CFO). The law requires exchange-traded public companies to file quarterly financial reports, referred to as Form 10-Qs, which set forth the company's financial condition. Such companies are also required to file more detailed reports, known as Form 10-Ks, on an annual basis.[44]

1. Executive certifications

The '34 Act and multiple SEC regulations set forth the specific contours of what public companies must include in their periodic filings. 18 U.S.C. § 1350, which was added to the federal criminal code in 2002 in the wake of the Enron scandal, imposes an additional requirement that carries stiff criminal penalties. The statute requires that each periodic report "shall be accompanied by a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer."[45] This signed, written statement must affirm that the reports comply with the '34 Act and that the information within the report "fairly presents, in all material respects, the financial condition and results of operations of the issuer."[46]

Significantly, there are two types of criminal penalties for violating this section. A willful violation, per 18 U.S.C. § 1350(c)(2), carries a statutory maximum sentence of 20 years' imprisonment and a $5 million fine.
18 U.S.C. § 1350(c)(1), which does not require willfulness and only requires knowledge, imposes a statutory maximum penalty of 10 years' imprisonment and a $1 million fine.

Few courts have confronted issues related to section 1350, though prosecutors have charged it on multiple occasions.[47] At least one district court has specifically upheld the statute's constitutionality.[48] Prosecutors are advised to consider section 1350 charges against senior officers, such as CEOs and CFOs, in accounting fraud cases. Often, in accounting fraud investigations, senior officers argue that they were distant from the actual problematic accounting at issue and relied on subordinate accountants to provide them with an accurate portrayal of the public company's books. Under these circumstances, where prosecutors may find it challenging to demonstrate specific intent, section 1350 may be appealing. Section 1350 counts offer an avenue for prosecution in sit-

---

44. Certain companies, including some foreign companies that issue in the United States, and companies whose shares are traded over the counter and not on exchanges, may be exempt from these reporting requirements.
45. 18 U.S.C. § 1350(a).
46. 18 U.S.C. § 1350(b).
47. *See, e.g.*, United States v. Wilson, 879 F.3d 795 (7th Cir. 2018) (affirming conviction that included section 1350 counts).
48. United States v. Scrushy, No. CR-03-BE-0530-S, 2004 WL 2713262 (N.D. Ala. Nov. 23, 2004). In United States v. Harra, 985 F.3d 196 (3d Cir. 2021), the Third Circuit vacated convictions in a complex securities fraud case that included section 1350 charges. The Third Circuit's opinion in *Harra* reflected questions about the falsity of the underlying certifications, but it did not specifically address the viability of section 1350 charges against culpable executives.

uations where a CEO or CFO has knowledge of the falsity of the books and records, even if they were not intimately involved in manipulative or fraudulent conduct.

2. Books and records

Section 13(b)(2) of the '34 Act imposes additional requirements on issuers. Specifically, it requires issuers to "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer," and to "devise and maintain a system of internal accounting controls."[49] The same statute provides that anyone who "knowingly circumvent[s] or knowingly fail[s] to implement a system of internal accounting controls or knowingly falsif[ies] any book, record, or account" is subject to criminal and civil penalties, though a criminal conviction requires a finding of willfulness.[50]

The books and records provision extends widely to almost any accounting entry that an issuer has, and each individual falsification constitutes its own crime. Significantly, a conviction on books and records does not require a showing of materiality. Individual accounting entries, if knowingly and willfully falsified, form the basis for a criminal charge even in the absence of an overarching scheme.

In *United States v. Armbruster*, the CFO of a publicly traded transportation company was convicted of two counts of falsifying an issuer's books and records.[51] *Armbruster* offers two lessons to prosecutors. First, Armbruster was convicted of two books and records counts, which together added up to $1 million in falsified assets on the public company's books. This amount paled in comparison to the fraud for which Armbruster was also convicted, which the indictment alleged cost shareholders hundreds of millions of dollars. The falsified entries in the issuer's books and records thus represented a small, but easily quantifiable, portion of the scheme. Second, as CFO of a large public company with multiple subsidiaries, Armbruster was convicted for causing the falsified entries pursuant to 18 U.S.C. § 2. Given the ambiguity in which employees often falsify or cause the falsified entries, prosecutors are advised to charge books and records violations using section 2.

Books and records charges may assist prosecutors in cases where the accounting fraud is difficult to parse fully or in other cases involving criminal conduct at issuers. For example, prosecutors often use books and records charges in Foreign Corrupt Practices Act (FCPA) cases.[52] The Criminal Division, Fraud Section, FCPA Unit, is available to provide guidance and support on such charges.

---

49. 15 U.S.C. § 78m(b)(2)(A)–(B).
50. *Id.* § 78m(b)(4).
51. 48 F.4th 527 (7th Cir. 2022) (affirming conviction).
52. 15 U.S.C. § 78m(b)(2)(A).

3. Misleading external auditors

Securities laws require that an external accounting firm audit all issuers' financial statements. Indeed, one of the takeaways of the Enron scandal was that Arthur Andersen had not managed to stop the massive accounting fraud scheme from unfolding despite its oversight. Because external auditors are usually unable to examine every line of a company's books and records, the SEC has promulgated a rule to penalize certain public company employees who take actions to manipulate, coerce, or mislead external auditors.

This rule, codified at 17 C.F.R. § 240.13b2–2(b)(1), prohibits an issuer's officers, directors, or any other person acting under their direction, from—

> directly or indirectly tak[ing] any action to coerce, manipulate, mislead, or fraudulently influence any independent public or certified public accountant engaged in the performance of an audit or review of the financial statements of that issuer that are required to be filed with the Commission pursuant to this subpart or otherwise if that person knew or should have known that such action, if successful, could result in rendering the issuer's financial statements materially misleading.[53]

Any lies or attempts to mislead a company's external auditors, if they could result in the issuer's financial statements being materially misleading, are usually sufficient to establish liability under this section. Prosecutors should consider using this charge where the evidence supports it, although this rule does not apply to junior employees or officers of subsidiaries, unless they are acting under the direction of a senior company officer.

In charging criminal violations of this rule, we note two points of caution. First, while paragraph (a) of the rule provides an alternative basis for liability—straightforward theories of false statements or omissions—we recommend charging deception of external auditors under paragraph (b). Paragraph (a) requires the false statements themselves to be material, whereas paragraph (b) merely requires that the person "knew or should have known that such action, if successful, could result in rendering the issuer's financial statements materially misleading."[54] This broader conception of materiality allows prosecutors to zoom out and contextualize the defendant's deceptive activity, considering the financial statements presented to shareholders as opposed to focusing on the materiality of an actual false statement itself.[55]

Second, we recommend focusing on the requisite intent. At least one appellate court has reversed a conviction under this rule where it found that the government's generalized evidence of intent was insufficient to support a

53. 17 C.F.R. § 240.13b2–2(b)(1).
54. *Id.*
55. There is also uncertainty surrounding the unit of prosecution for violations of paragraph (a). *See* United States v. Turner, No. CR05-355C, 2007 WL 983124, at *5 (W.D. Wash. Mar. 26, 2007).

conviction.[56] The plain and broad reading of this rule invites its use, but the government is always required to establish proof of willfulness, which can be challenging in criminal cases.

C. Misappropriation of information and insider trading under the commodities laws

Before Dodd–Frank, the CEA prohibited insider trading involving the misuse of nonpublic information by personnel of the CFTC, exchanges, and self regulatory organizations, but it did not provide generally applicable authority prohibiting such misconduct.

In addition, the differences between the securities and commodities markets, and missions of the SEC and CFTC in overseeing these respective markets, impact the evaluation of the propriety of the use of nonpublic information. The securities markets focus on capital formation, and the laws address transparency and corporate duties to disclose material information to protect shareholders. The derivatives markets have operated to allow market participants to trade based on lawfully obtained material nonpublic information to facilitate management and transfer of risk, including price discovery and hedging or protecting against risks in commodity positions.

With the new anti-fraud and manipulation provisions under Dodd–Frank and the CFTC's Rule 180.1, the CFTC recognized that, in addition to misuse of nonpublic information by government personnel,[57] there may be a violation by "trading on the basis of material nonpublic information in breach of a pre-existing duty (established by another law or rule, or agreement, understanding, or some other source), or by trading on the basis of material nonpublic information that was obtained through fraud or deception."[58]

In recent years, the CFTC has brought civil enforcement actions under these provisions for improper trading based on the illegal misappropriation of nonpublic information.[59] In doing so, it applied the misappropriation theory of insider trading that has been applied in the securities context.[60]

---

56. United States v. Goyal, 629 F.3d 912 (9th Cir. 2010).
57. The prior insider trading provision was also expanded under Dodd–Frank. *See* 7 U.S.C. § 6c(a)(4)(A).
58. Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,398, 41,403 (July 14, 2011).
59. *In re* Motazedi, CFTC No. 16-02 (Dec. 2, 2015); *In re* Ruggles, CFTC No. 16-34 (Sept. 29, 2016); Memorandum Opinion and Order, CFTC v. EOX Holdings LLC, No. 19-cv-2901 (S.D. Tex. Sept. 26, 2019), ECF No. 74.
60. *See* CFTC v. EOX Holdings LLC, 405 F. Supp. 3d 697, 710–11 (S.D. Tex. Sept. 26, 2019) (applying the misappropriation theory recognized in the securities context in United States v. O'Hagan, 521 U.S. 642 (1997)).

In *United States v. Marcus Schultz*,[61] the Department brought the first criminal case involving insider trading in the commodities markets under these provisions. In this and related cases, energy traders and brokers illegally misappropriated material nonpublic information in breach of their duties of confidentiality, loyalty, and trust for use in prearranged fraudulent and other prohibited trades for their personal gain. The members of the scheme also engaged in other illegal conduct to conceal the fraudulent activity and related illicit profits, including lying to the CFTC and relevant exchange. In addition, certain members of the scheme coordinated paying and receiving illegal kickbacks, whereby certain traders received a portion of the commissions that their employer paid the brokerage firm executing their trades.

Defendant Schultz pleaded guilty to conspiracy to violate the CEA (7 U.S.C. §§ 6c(a), 9(1), 13(a)(2), 13(a)(5)) and Rule 180.1 thereunder and wire fraud (18 U.S.C. § 1343).[62] Subsequently, the Department announced additional charges and guilty pleas by other traders and a broker involved in the scheme, which included not only commodities fraud, wire fraud, and related conspiracy charges, but also charges for honest services fraud for those involved in the illegal kickback activity.[63] The CFTC resolved parallel enforcement actions. The case against Defendant Matthew Clark, a trader indicted in February 2022 for participating in the insider trading scheme and kickback activity, remains pending as of this article's date of publication.[64]

In these cases, the breach of a recognized duty was established based on employer–employee or broker–customer relationships and the applicable agreements, policies and procedures, exchange rules, CFTC regulations, and other applicable laws. The material nonpublic information that was misappropriated included the following: identity, trade interests, and other terms and conditions of the trading activity, including prices, purchase or sale, quantity, volume, source, delivery points, timing, and thresholds or limits to the terms to which the customer would agree. Notably, in these cases, the Department not only relied upon the CEA anti-fraud provisions and Rule 180.1, but also upon the statutory provision prohibiting prearranged trades. Even though the misappropriated information was used to coordinate fictitious, prearranged trades at issue, such violations did not require the government to establish that nonpublic information was misappropriated in violation of an established duty. As discussed above, pursuing multiple charging theories is advisable given the lack of precedent in this area.

---

61. Information, United States v. Schultz, No. 4:20-cr-270 (S.D. Tex. June 29, 2020), ECF No. 1. The case was brought with a CFTC parallel action. *See In re* Marcus Schultz, CFTC No. 20-76 (Sept. 30, 2020); *see also In re* Classic Energy LLC and Mathew D. Webb, CFTC No. 19-50 (Sept. 30, 2019).
62. Signed Plea Agreement, *Schultz*, No. 4:20-cr-270, ECF No. 19.
63. *See* United States v. James, No. 20-cr-695 (S.D. Tex.); United States v. Webb, No. 21-cr-233 (S.D. Tex.); United States v. Tippett, No. 21-cr-364 (S.D. Tex.); United States v. Miller, No. 21-cr-570 (S.D. Tex.).
64. Indictment, United States v. Clark, No. 22-cr-55 (S.D. Tex. Feb. 3, 2022), ECF No. 1.

IV. Conclusion

New types of fraud and manipulation are constantly emerging in the securities and commodities markets, particularly as our financial markets evolve with developing technology and types of financial products. As a result, prosecutors need flexibility in how to combat and prosecute this illegal activity. This article provides a helpful resource for prosecutors to rely upon in understanding the applicable frameworks and bringing important cases to combat all types of financial fraud and sophisticated economic crimes and to protect our markets, investors, and other market participants.

About the Authors

Justin Weitz served as the Acting Principal Assistant Chief of the Market Integrity and Major Frauds Unit, Criminal Division, Fraud Section, from 2020 to 2022.

Jennifer Farer is a Trial Attorney in the Market Integrity and Major Frauds Unit of the Fraud Section, Criminal Division, where she focuses on prosecuting complex securities, commodities, government procurement, and other financial fraud cases. During her time in the Fraud Section, Jennifer completed a detail at the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, where she served as a Senior Advisor to the Enforcement Division and then Assistant Chief Counsel for Litigation and Enforcement. Jennifer was previously in private practice where she represented companies and individuals in criminal and civil enforcement cases, internal investigations, and complex litigation and class actions, as well as advised clients on regulatory compliance.

The Foreign Corrupt Practices Act: Continued Progress in the Fight Against Corruption

David I. Salem
Assistant U.S. Attorney
District of Maryland

Derek J. Ettinger
Assistant Chief, FCPA Unit
Criminal Division, Fraud Section

I. History of the FCPA

The Foreign Corrupt Practices Act (FCPA)[1.] was first enacted in the wake of the Watergate scandal that led to President Richard Nixon's resignation and resulted in a dramatic plunge in Americans' overall trust in government. In 1976, following certain prosecutions for illegal use of corporate funds arising out of the Watergate scandal, the U.S. Securities and Exchange Commission (SEC) issued a *Report on Questionable and Illegal Corporate Payments and Practices.* In its report, the SEC determined that U.S. corporations were using secret "slush funds" for various purposes, including illegal campaign contributions in the United States and bribes to foreign officials abroad.[2.]

The FCPA was thus enacted in 1977 for the purpose of making it unlawful for certain classes of persons and entities to make corrupt payments to foreign government officials to assist in obtaining or retaining business.

In 1998, Congress amended the FCPA and expanded its scope to (1) include payments made to secure "any improper advantage"; (2) reach certain foreign persons who commit an act in furtherance of a foreign bribe while in the United States; (3) cover public international organizations in the definition of "foreign official"; (4) add an alternative basis for jurisdiction based on nationality; and (5) apply criminal penalties to foreign nationals employed by or acting as agents of U.S. companies.[3.] The FCPA also contains accounting provisions applicable

1. Foreign Corrupt Practices Act of 1977 (FCPA), Pub. L. No. 95-213, 91 Stat. 1494 (codified as amended at 15 U.S.C. §§ 78dd-1, *et seq.*).
2. U.S. Sec. & Exch. Comm'n, Report of the Securities and Exchange Commission on Questionable and Illegal Corporate Payments and Practices 2–3 (1976); U.S. Dep't of Just. & Sec. & Exch. Comm'n, A Resource Guide to the U.S. Foreign Corrupt Practices Act 2 (2d ed. 2020) [hereinafter FCPA Resource Guide].
3. *See* International Anti-Bribery and Fair Competition Act of 1998, Pub. L. No. 105-366, 112 Stat. 3302 (1998); *see also* S. Rep. No. 105-277, at 2–3 (1998) (describing amendments to "the FCPA to conform it to the requirements of and to implement the OECD Convention").

to public companies.[4]

Congress viewed the FCPA's passage as critical to stopping corporate bribery, which had tarnished the image of U.S. businesses, impaired public confidence in the financial integrity of U.S. companies, and hampered the efficient functioning of the markets.[5] Two of the law's chief purposes, therefore, were to level the playing field for honest businesses and restore public confidence in the integrity of the marketplace.[6]

In the more than 40 years since Congress passed the FCPA, significant progress has been made in the global fight against corruption. For example, the United States and other countries are parties to various international anti-corruption conventions in which the parties undertake commitments to adopt a range of preventive and criminal law measures to combat corruption.[7]

The growing international coalition to fight corruption is also reflected in a recent trend in FCPA enforcement, namely, the increase in international

---

4. Section 13(b)(2)(A)–(B) of the Exchange Act (codified at 15 U.S.C. § 78m(b)(2)(A)–(B)). These accounting provisions, which Congress designed to operate in tandem with the anti-bribery provisions of the FCPA, prohibit off-the-books accounting. They require companies covered by the provisions to (a) "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect" an issuer's transactions and dispositions of an issuer's assets; and (b) "devise and maintain a system of internal accounting controls sufficient to" assure management's control, authority, and responsibility over the firm's assets. *Id.*

5. *See* H.R. Rep. No. 95-640, at 4–5 (1977); S. Rep. No. 95-114, at 3–4 (1977).

6. *See* FCPA Resource Guide, *supra* note 2, at 1–2; H.R. Rep. No. 95-640, at 4–5 (1977). The House Report made clear Congress's concerns:

> The payment of bribes to influence the acts or decisions of foreign officials, foreign political parties or candidates for foreign political office is unethical. It is counter to the moral expectations and values of the American public. But not only is it unethical, it is bad business as well. It erodes public confidence in the integrity of the free market system. It short-circuits the marketplace by directing business to those companies too inefficient to compete in terms of price, quality or service, or too lazy to engage in honest salesmanship, or too intent upon unloading marginal products. In short, it rewards corruption instead of efficiency and puts pressure on ethical enterprises to lower their standards or risk losing business.

Id.

7. FCPA Resource Guide, *supra* note 2, at 6–7. *See, e.g.*, Organisation for Econ. Co-operation and Dev., Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, at art. 1.1 (1997) [hereinafter Anti-Bribery Convention]. The Anti Bribery Convention requires member countries to make it a criminal offense "for any person intentionally to offer, promise or give any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business." *Id.*

cooperation as well as the coordination of corporate resolutions with other countries. Such coordination helps avoid imposing duplicative penalties, forfeiture, and disgorgement for the same illicit conduct.[8] It also allows companies to obtain resolutions with multiple jurisdictions conducting parallel investigations pursuant to separate anti-corruption laws. As part of these coordinated

8. Since 2008, the Department has coordinated resolutions with foreign authorities in more than 10 cases. *See* FCPA Resource Guide, *supra* note 2, at 71. *See, e.g.*, Press Release, U.S. Dep't of Just., Glencore Entered Guilty Pleas to Foreign Bribery and Market Manipulation Schemes (May 24, 2022) (United States v. Glencore International AG, Department coordinating with United Kingdom, Brazil, and Switzerland); Press Release, U.S. Dep't of Just., Vitol Inc. Agrees to Pay over $135 Million to Resolve Foreign Bribery Case (Dec. 3, 2020) (United States v. Vitol Inc., Department coordinating with Brazil); Press Release, U.S. Dep't of Just., Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case (Jan. 31, 2020) (United States v. Airbus, Department coordinating with France and United Kingdom); Press Release, U.S. Dep't of Just., TechnipFMC Plc and U.S.-Based Subsidiary Agree to Pay over $296 Million in Global Penalties to Resolve Foreign Bribery Case (June 25, 2019) (United States v. TechnipFMC, Department coordinating with Brazil); Press Release, U.S. Dep't of Just., Société Générale S.A. Agrees to Pay $860 Million in Criminal Penalties for Bribing Gaddafi-Era Libyan Officials and Manipulating LIBOR Rate (June 4, 2018) (United States v. Société Générale, Department coordinating with France); Press Release, U.S. Dep't of Just., Keppel Offshore & Marine Ltd. and U.S. Based Subsidiary Agree to Pay $422 Million in Global Penalties to Resolve Foreign Bribery Case (Dec. 22, 2017) (United States v. Keppel Offshore & Marine Ltd., Department coordinating with Brazil and Singapore); Press Release, U.S. Dep't of Just., SBM Offshore N.V. and United States-Based Subsidiary Resolve Foreign Corrupt Practices Act Case Involving Bribes in Five Countries (Nov. 29, 2017) (United States v. SBM Offshore, Department coordinating with the Netherlands and Brazil); Press Release, U.S. Dep't of Just., Telia Company AB and Its Uzbek Subsidiary Enter into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan (Sept. 21, 2017) (United States v. Telia Company AB, Department and SEC coordinating with the Netherlands); Press Release, U.S. Dep't of Just., Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case (Jan. 17, 2017) (United States v. Rolls- Royce plc, No. 16-cr-247 (S.D. Ohio Jan. 17, 2017), Department coordinating with United Kingdom and Brazil); Press Release, U.S. Dep't of Just., Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016) (United States v. Odebrecht S.A., No. 16-cr-643, Department coordinating with Brazil and Switzerland); Press Release, U.S. Dep't of Just., Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016) (United States v. Braskem S.A., Department and SEC coordinating with Brazil and Switzerland); Press Release, U.S. Dep't of Just., VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme (Feb. 18, 2016) (United States v. VimpelCom Ltd., Department and SEC coordinating with the Netherlands); Press Release, U.S. Dep't of Just., Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines (Dec. 15, 2008) (United States v. Siemens AG, Department and SEC coordinating with Germany).

resolutions, the Department of Justice (Department) has often credited fines, penalties, forfeiture, and disgorgement that a resolving company pays to foreign authorities for overlapping conduct.[9.]

II. The Prosecution of *United States v. Lambert*

In part because of their international dimension and financial complexity, FCPA investigations and trials present some unique challenges. The prosecution of *United States v. Mark Lambert*, tried in the District of Maryland in 2019, illustrates some of those challenges.[10.]

The case centered around bribes paid to a foreign official and national of the Russian Federation named Vadim Mikerin. From approximately 2004 to 2011, Mikerin was the Director of the Russian company JSC Techsnabexport (TENEX). TENEX, an agency and instrumentality of the Russian Federation, supplied uranium and uranium enrichment services to nuclear power companies throughout the world on behalf of the Russian government. Mikerin later became President of TENEX's wholly-owned U.S. subsidiary, TENAM Corporation (TENAM).[11.]

In 2014, agents from the Federal Bureau of Investigation and the Department of Energy's (DOE) Office of the Inspector General executed a search warrant at Mikerin's office in Bethesda, Maryland. The agents found documents and laptop computers in a locked safe (and in other locations) that they were able to access during the search.

In part through executing the search warrant and subsequent investigative steps, the agents obtained information that helped expose a complex bribery scheme involving Mikerin and a Maryland based company called Transport Logistics International (TLI).

In October 2014, agents approached and interviewed Mikerin, who was then arrested.[12.] Mikerin ultimately admitted that, among other things, he had participated in a sophisticated money-laundering conspiracy to promote a multi-year bribery scheme, whereby he conspired with executives at TLI to make—and act as intermediaries for—corrupt payments for his benefit to offshore shell companies around the world.[13.] In particular, he admitted to a scheme in which TLI, in order to benefit and influence Mikerin, wired more

9. FCPA Resource Guide, *supra* note 2, at 71. This practice of coordinating resolutions to avoid "piling on" is memorialized in the Justice Manual, which instructs prosecutors to "endeavor, as appropriate, to coordinate with and consider the amount of fines, penalties, and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct." Justice Manual 1-12.100.

10. United States v. Lambert, No. 20-4590, 2022 WL 2871909 (4th Cir. July 21, 2022) (affirming district court and upholding Lambert's conviction).

11. *See* Second Superseding Indictment at 3, United States v. Lambert, No. 18-cr-12 (D. Md. May 22, 2019), ECF No. 79.

12. *See, e.g.*, Defendant's Motion to Suppress, United States v. Mikerin, No. 14-cr-529 (D. Md. Mar. 13, 2015), ECF No. 46.

13. Superseding Information at 4, *Mikerin*, No. 14-cr-529, ECF No. 98.

than $1.5 million from its bank account in Maryland to three shell companies registered in the Seychelles, British Virgin Islands, and the United Kingdom, with bank accounts in the Republic of Cyprus, the Republic of Latvia, and Switzerland.[14] Mikerin pleaded guilty in the District of Maryland to one count of conspiracy to commit money laundering regarding the scheme.[15] In March 2018, TLI entered into a deferred prosecution agreement with the Fraud Section of the Department's Criminal Division and the U.S. Attorney's Office for the District of Maryland, in which TLI admitted to conspiring to violate the FCPA.[16]

As detailed during the trial, executives from TLI made bribe payments for the benefit of Mikerin in order to enrich themselves corruptly and criminally. They also understood that the bribes would allow them to win sole-source contracts with TENEX to transport uranium to and from Russia,[17] including uranium involved in the historic 1993 HEU–LEU Agreement. That agreement, colloquially known as the United States–Russian "Megatons to Megawatts" Agreement or the "Swords to Plowshares" Agreement, was designed to decrease the number of nuclear weapons that remained in Russia after the fall of the Soviet Union, while simultaneously creating nuclear energy that could be used in the United States.[18] In essence, Russia agreed to take weapons-grade uranium—uranium that was in its nuclear weapons—and down-blend it, making it less powerful or less concentrated. The United States, in turn, agreed to buy that uranium from Russia to use for fuel in American nuclear power plants.[19]

The Megatons to Megawatts Agreement accounted for the down blending of approximately 500 metric tons of weapons grade uranium to low enriched uranium (LEU).[20] That is the equivalent of roughly 20,000 nuclear weapons taken out of circulation.[21] By some estimates, by 2008, approximately 1 in

14. Attachment A: Stipulated Facts, *Mikerin*, No. 14-cr-529, ECF No. 103-1; Transcript of Trial, Nov. 14, 2019, at 105:8–16, 107:2–8, *Lambert*, No. 18-cr-12, ECF No. 251 [hereinafter Nov. 14 *Lambert* Trial Transcript].
15. Plea Agreement at 1, *Mikerin*, No. 14-cr-529, ECF No. 103.
16. *See* Press Release, U.S. Dep't of Just., Transport Logistics International Inc. Agrees to Pay $2 Million Penalty to Resolve Foreign Bribery Case (Mar. 13, 2018); Deferred Prosecution Agreement, United States v. Transport Logistics Int'l, Inc., No. 18-cr-11 (D. Md. Mar. 12, 2018), ECF No. 6.
17. Transcript of Trial (Morning Session), Nov. 4, 2019, at 145:12–20, *Lambert*, No. 18-cr-12, ECF No. 246 [hereinafter Nov. 4 Morning *Lambert* Trial Transcript]; Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 129:8–15.
18. Transcript of Jury Trial P.M. Proceedings, Oct. 30, 2019, at 32:4–32:25, *Lambert*, No. 18-cr-12, ECF No. 140 [hereinafter Oct. 30 Afternoon *Lambert* Trial Transcript].
19. Nov. 4 Morning *Lambert* Trial Transcript, *supra* note 17, at 102; *Megatons to Megawatts*, U.S. Enrichment Corp., https://web.archive.org/web/20140113070126/http://www.usec.com/russian-contracts/megatons-megawatts (archived Jan. 13, 2014) (last visited Sept. 14, 2022).
20. Oct. 30 Afternoon *Lambert* Trial Transcript, *supra* note 18, at 32:18–25.
21. *Id.*; U.S. Enrichment Corp., *supra* note 19.

10 "American homes, businesses, schools and hospitals receive[d] electricity generated by fuel fabricated using LEU from the Megatons to Megawatts program."[22]

A program of such immense scale required shipping a massive amount of uranium. In particular, it required first transporting the uranium out of Russia and to the United States and then returning another type of low-grade uranium called "feed" back to Russia. TLI won the contracts to move the uranium from Russia to the United States.[23] As detailed during the trial, through the bribery scheme, TLI also won the contracts to transport the low grade uranium—the feed—back to Russia.[24] Once the scheme was up and running, the evidence presented at trial showed that TLI continued to pay bribes to win TENEX business on subsequent commercial contracts.

The conspirators thus violated the anti-bribery provisions of the FCPA and corrupted the extraordinarily sensitive process of transporting nuclear fuel to and from the United States.

Two corporate executives at TLI—Daren Condrey and Mark Lambert—were charged. Another executive who had been involved in the scheme died before the case was indicted.[25] Condrey pleaded guilty and agreed to cooperate against Lambert, who went to trial in Greenbelt, Maryland, in the fall of 2019. Lambert was part-owner and co-president of the corporation. He was charged with one count of conspiracy to violate the FCPA and to commit wire fraud, seven counts of substantive FCPA violations, two counts of wire fraud, and one count of money laundering.[26] Following a three-week trial, the jury found Lambert guilty of conspiracy, four counts of violating the FCPA, and two counts of wire fraud.[27] The U.S. District Court sentenced Lambert to four years in prison, three years supervised release, a $20,000 fine, and a $700 special assessment.

A. Gathering evidence

As the evidence at trial demonstrated, the conspirators were particularly diligent about disguising the bribe scheme. For example, TLI's executives hid the scheme by creating fake invoices that looked like they were coming from TENEX and by falsely recording the bribe payments in their corporate books.[28] Initially, they falsely recorded the bribes as "commissions," but realized before long that referencing the payments as "commissions" would raise

22. U.S. Enrichment Corp., *supra* note 19; *see also* Oct. 30 Afternoon *Lambert* Trial Transcript, *supra* note 18, at 33:1–4.
23. Nov. 4 Morning *Lambert* Trial Transcript, *supra* note 17, at 107:3–10.
24. *Id.*
25. *Id.* at 92:24–25, 131:24–25.
26. *See generally* Second Superseding Indictment, *supra* note 11.
27. *See* Press Release, U.S. Dep't of Just., Former President of Transportation Company Found Guilty of Violating the Foreign Corrupt Practices Act and Other Crimes (Nov. 22, 2019).
28. Nov. 4 Morning *Lambert* Trial Transcript, *supra* note 17, at 147.

too many questions.[29] So they switched to recording the bribes as "remuneration," a term that referred to legitimate discount programs that TLI used with certain customers based in Asia.[30] As part of the scheme, the TLI conspirators hoped that TLI employees and other individuals conducting oversight from TLI's parent company would incorrectly assume that the bribes to Mikerin, which were falsely labeled "remuneration," were simply part of a discount given to TENEX.[31] The co-conspirators also tracked the corrupt and fraudulent payments on internal spreadsheets that they shared with each other.[32]

The TLI executives emailed directly with Mikerin at Mikerin's personal and pseudonymous email account where he went by the alias "Marvin Jodel."[33] In those private communications, Mikerin and his co-conspirators used code words like "lucky figure," "LF," and "cake" when discussing and arranging the bribe payments to Mikerin.[34]

As Lambert's trial demonstrated, emails and other electronic communications can provide significant evidence demonstrating the guilt of individuals engaged in a bribery scheme, as well as other criminal conduct, and their participation in a complex conspiracy. The evidence at trial included electronic communications from both personal and corporate email accounts,[35] all of which helped the government reconstruct and understand the full scope of the conspiracy. Electronic evidence also corroborated the corrupt intent of the members of the conspiracy, in part because, when discussing bribes, the co-conspirators generally used Mikerin's personal email address with the alias "Marvin Jodel" rather than his TENEX or TENAM email account,[36] and also referred to the so-called "remuneration" (that is, the bribes) by using code words.[37] The trial evidence even included an iMessage between Condrey and Lambert, in which they discussed who at TENEX besides Mikerin knew about "LF," an acronym used to designate "Lucky Figures," or bribes paid to Mikerin.[38]

As with many criminal trials, having a cooperator who can explain the manner and means of the conspiracy and the "backroom conversations" of the conspirators can serve as very valuable evidence. In the *Lambert* trial, Daren Condrey testified as a cooperating witness and explained the internal documents and other evidence that demonstrated the bribery scheme and

29. *Id.* at 148.
30. *Id.*; Transcript of Trial (Morning Session), Nov. 5, 2019, at 55–57, *Lambert*, No. 18-cr-12, ECF No. 247 [hereinafter Nov. 5 Morning *Lambert* Trial Transcript].
31. *See* Transcript of Jury Trial Proceedings (Afternoon Session), Nov. 4, 2019, at 10, *Lambert,* No. 18-cr-12, ECF No. 183.
32. *Id.* at 27–29, 123.
33. Nov. 5 Morning *Lambert* Trial Transcript, *supra* note 30, at 79–80.
34. Nov. 4 Morning *Lambert* Trial Transcript, *supra* note 17, at 148–49.
35. *See, e.g.*, Nov. 5 Morning *Lambert* Trial Transcript, *supra* note 30, at 74–75, 79:16–20.
36. *Id.* at 81.
37. *Id.* at 93:23–94:7.
38. *Id.* at 106–10, Ex. 76.

the conspirators' efforts to conceal the bribe payments to Mikerin.[39] Through Condrey's testimony and other evidence, the jury learned about the origin and nature of the scheme, the methods used to conceal it, and the various coded documents that tracked the bribes and hid them from prying eyes.[40]

In addition to electronic evidence and the testimony of cooperators, cases such as *Lambert* typically include the use of Mutual Legal Assistance Treaties (MLATs) or other methods to gather evidence from foreign authorities. Because obtaining foreign-based evidence can be a valuable component to a successful FCPA prosecution and simultaneously extremely time-consuming, prosecutors should consider seeking a tolling order under 18 U.S.C. § 3292 when appropriate.

In *Lambert*, besides the bank records from TLI's Maryland bank showing that TLI wired payments to the shell companies, the government also introduced evidence obtained pursuant to three separate MLAT requests, which included the foreign bank records of the accounts into which TLI paid the bribes.[41] At trial, part of Lambert's defense centered on his counsel's arguments that the payments he authorized were merely purported discounts for TENEX.[42] The evidence, however, showed that the shell companies that were paid had nothing to do with TENEX. The evidence obtained through MLAT requests included, for example, (1) the registration documents of the offshore companies, revealing that none conducted any obvious nuclear industry related work;[43] (2) evidence that one of the shell companies was involved in, among other things, electrical appliances, textiles, and clothes;[44] and (3) evidence that another shell company was involved in metal trading.[45] There was thus ample evidence suggesting that, contrary to the defense arguments, none of the shell companies that Lambert and his co-conspirators paid at Mikerin's direction were actually subsidiaries of, or otherwise related to, TENEX.

B. Proving the elements of the offense

In *Lambert*, the district court instructed the jury that to find the defendant guilty of violating the FCPA, the government needed to prove the following elements beyond a reasonable doubt: (1) that Lambert was a "domestic concern or an officer, director, employee or agent of a domestic concern or a stockholder thereof acting on behalf of such domestic concern"; (2) that Lambert "acted corruptly and willfully"; (3) that Lambert "made use of the mails or any means or instrumentality of interstate commerce in furtherance of conduct that violates the FCPA"; (4) that Lambert "either paid or offered, promised

39. *See, e.g., id.* at 42:19–52:25.
40. *Id.* at 75:12–16.
41. Transcript of Jury Trial A.M. Proceedings, Nov. 7, 2019, at 165:7–167:17, *Lambert*, ECF No. 149 [hereinafter Nov. 7 Morning *Lambert* Trial Transcript].
42. Transcript of Trial (Morning Session), Oct. 30, 2019, at 24–25, *Lambert*, ECF No. 245.
43. Nov. 7 Morning *Lambert* Trial Transcript, *supra* note 41, at 170:7–174:18.
44. *Id.* at 172:14–17.
45. *Id.* at 174:17–18.

or authorized the payment of money or of anything of value"; (5) "that the payment was either to a foreign official or to any person while [Lambert] knew that all or a portion of the payment would be offered, given or promised directly or indirectly, to a foreign official"; (6) "that the payment was for one of four purposes[: (a) t]o influence any act or decision over the foreign official in his or her official capacity," (b) "to induce the foreign official to do or omit to do any act in violation of that official's lawful duty," (c) "to induce that foreign official to use his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality[,] or" (d) "to secure any improper advantage"; and (7) "that the payment was made to assist [Lambert] in obtaining or retaining business for or with[,] or directing business to[,] any person."[46]

An analysis of each element of an FCPA violation would take us far beyond the scope of this article, but some examples of typical issues that arise are explained below.

1. Element one

The first requirement is to show that the FCPA covers the charged individual. Lambert was charged under 15 U.S.C. § 78dd-2, which requires, *inter alia*, that an individual be a "domestic concern," or an officer, director, employee, or agent of a "domestic concern." The statute defines a "domestic concern" as (a) "any individual who is a citizen, national or resident of the United States" or (b) "any corporation, partnership, association, joint stock company, business trust, unincorporated organization[,] or sole proprietorship which has its principal place of business in the United States[,] or which is organized under the laws of a state of the United States or a territory, possession[,] or commonwealth of the United States."[47]

Because Lambert was both a U.S. citizen and an officer and employee of a company with its principal place of business in Maryland (that is, a company that was itself a domestic concern), this element was not seriously in dispute.

In other circumstances, the analysis of the first element may be more complicated. For example, a bribe-paying intermediary whom a company engages either officially or unofficially may neither be a domestic concern nor an officer, director, or employee of a domestic concern (or "issuers" of stock on U.S. exchanges). The FCPA can, nonetheless, cover such third parties as agents of a domestic concern or issuer. Moreover, under traditional principles of respondeat superior, a company can be liable for the acts of its agents undertaken within the scope of their employment and intended, at least in part, to benefit the company.[48]

In addition, under 15 U.S.C. § 78dd-3, a foreign national can also be prose-

46. Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 54–55.
47. 15 U.S.C. § 78dd-2(h)(1)(A); Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 55.
48. FCPA Resource Guide, *supra* note 2, at 28; *see, e.g.*, Standard Oil Co. v. United States, 307 F.2d 120, 127 (5th Cir. 1962).

cuted under the FCPA if he or she acts in furtherance of a corrupt payment (or an offer, promise, or authorization to pay) while in the territory of the United States. For example, assuming the other elements were satisfied, the FCPA could cover a foreign national with no employment or agency connection to a domestic concern or issuer if she came to the United States and offered a bribe to a foreign official or delivered a cash bribe in the United States for the benefit of a foreign official.[49]

A foreign company or individual may also be held liable for aiding and abetting an FCPA violation or for conspiring to violate the FCPA, even if the foreign company or individual did not act in furtherance of the scheme while in the territory of the United States. When prosecuting a conspiracy case, the United States generally has jurisdiction over all conspirators if at least one of them is an issuer or a domestic concern, or commits a reasonably foreseeable overt act within the United States. The same principle applies to aiding and abetting violations.[50]

2. Element four

The fourth element is worth pausing on briefly. The FCPA is explicit that it is not necessary for a bribe payment to occur to violate the statute. It also specifically prohibits an offer or promise to pay a bribe as well as authorizing a bribe payment. In addition to presenting evidence of the bribe payments themselves, the government in *Lambert* put on evidence that Lambert and Condrey offered or promised bribe payments and authorized those payments. That evidence would have been legally sufficient to secure a guilty verdict even absent any evidence that the payments had ever been made.[51] As a practical matter, however, the evidence in *Lambert* established all the above.

3. Element five

To prove an FCPA violation, the government must also prove that the offer, promise, payment, or authorization of payment was to a foreign official, or to any person whom the defendant knew would directly or indirectly offer, give, or promise all or a portion of that payment to a foreign official (that is, a third-party intermediary). When a foreign government is organized

---

49. 15 U.S.C. § 78dd-3.

50. FCPA Resource Guide, *supra* note 2, at 36. *See* United States v. MacAllister, 160 F.3d 1304, 1307 (11th Cir. 1998); United States v. Winter, 509 F.2d 975, 982 (5th Cir. 1975).*But see* United States v. Hoskins, 902 F.3d 69, 76–97 (2d Cir. 2018) (holding that an individual can be prosecuted criminally for conspiracy to violate the FCPA anti-bribery provisions or for aiding and abetting an FCPA anti-bribery violation only if that individual's conduct and role fall into one of the specifically enumerated categories expressly listed in the FCPA's anti-bribery provisions); Memorandum Opinion and Order, United States v. Rafoi-Bleuler, No. 17-cr-514 (S.D. Tex. Nov. 10, 2021), ECF No. 255 (following *Hoskins*, but currently on appeal in the 5th Circuit). But *cf.* United States v. Firtash, 392 F. Supp. 3d 872, 889–92 (N.D. Ill. 2019) (rejecting the reasoning in the *Hoskins* decision).

51. Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 58:12–17.

similar to the U.S. system, what constitutes a government official is typically clear, such as an executive-level official like a president, governor, or minister of energy or transportation. Governments, however, can be organized in very different ways.[52] For example, "[m]any operate through state-owned and state-controlled entities, particularly in such areas as aerospace and defense manufacturing, banking and finance, healthcare and life sciences, energy and extractive industries, telecommunications, and transportation."[53] Thus, in some instances, determining whether the bribe payee was a foreign official for purposes of the statute requires understanding how the foreign government is organized and how it functions.

In part to account for this variability in government organization, the FCPA includes officers or employees of agencies and instrumentalities within the definition of "foreign official."[54] Specifically, the FCPA defines a "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization."[55]

The term "instrumentality" is broad and can include state-owned or state-controlled entities like TENEX and TENAM. Whether a particular entity constitutes an "instrumentality" under the FCPA requires a fact-specific analysis of an entity's ownership, control, status, and function.[56]

Lambert provides a useful illustration. ROSATOM, the parent company of TENEX, was essentially the equivalent of the U.S. DOE.[57] Mikerin worked for ROSATOM's commercial subsidiary TENEX and later TENEX's American subsidiary TENAM. As the district court instructed, the government needed

---

52. *See* FCPA Resource Guide, *supra* note 2, at 19–20. Additionally, during the period surrounding the FCPA's adoption, state-owned entities held virtual monopolies and operated under state-controlled price-setting in many national industries around the world. *See* The World Bank Grp., Bureaucrats in Business: The Economics and Politics of Government Ownership 78 (1995); Sunita Kikeri and Aishetu Kolo, The World Bank Grp., State Enterprises (2006).

53. Kikeri & Kolo,*supra* note 52, at 1 ("[A]fter more than two decades of privatization, government ownership and control remains widespread in many regions—and in many parts of the world still dominates certain sectors."); FCPA Resource Guide, *supra* note 2, at 20.

54. FCPA Resource Guide, *supra* note 2, at 20.

55. 15 U.S.C. § 78dd-2(h)(2)(A). Another way to qualify as a "foreign official" under the statute is to "act[] in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." *Id.*

56. FCPA Resource Guide, *supra* note 2, at 20. To date, consistent with the Department's approach, all district courts that have considered this issue have concluded that it is an issue of fact for a jury to decide. See Order, United States v. Carson, No. 09-cr-77 (C.D. Cal. May 18, 2011), ECF No. 373; United States v. Aguilar, 783 F. Supp. 2d 1108 (C.D. Cal. 2011); Order, United States v. Esquenazi, No. 09-cr-21010 (S.D. Fla. Aug. 5, 2011), ECF No. 309; *see also* Management Order, United States v. O'Shea, No. 09-cr-629 (S.D. Tex. Jan. 3, 2012), ECF No. 142; Order, United States v. Nguyen, No. 08-cr-522 (E.D. Pa. Dec. 30, 2009), ECF No. 144.

57. Oct. 30 Afternoon *Lambert* Trial Transcript, *supra* note 18, at 21:9–11.

to prove that either of these entities was an instrumentality of the Russian government such that Mikerin qualified as a foreign official.[58]

The Eleventh Circuit addressed what qualifies as an "instrumentality" under the FCPA in *United States v. Esquenazi,* a case involving a state-owned Haitian telecommunications company.[59] The Eleventh Circuit concluded that an "instrumentality" under the FCPA is "an entity controlled by the government of a foreign country that performs a function the controlling government treats as its own."[60] Although the court noted that this test is a fact-bound inquiry, it provided a non-exhaustive list of factors to determine (1) whether the government controls an entity, and another list of non-exhaustive factors to determine (2) whether the entity performs a function that the government treats as its own.[61]

In addition, several courts in other circuits, including the court in *Lambert*, have approved final jury instructions providing a similar non-exclusive list of factors to be considered.[62] It is important for prosecutors to tailor the factors to their particular case and to urge the court to include them in its instructions. In drafting this instruction, it is useful to draw on cases from the districts that have taken FCPA prosecutions to verdict. In the District of Maryland, for example, the district judge requested that the government offer its version of the instructions with each sentence footnoted to where that instruction was previously given, or to such other authority as would justify the language used.[63] In *Lambert,* the following factors were included in the instructions for the jury's consideration:

Control

1. The Russian government's formal designation of the entity as a government-owned entity;

2. The circumstances under which the entity was created;

3. Whether the Russian government had a majority or controlling interest in TENEX or TENAM, including whether it provides financial support such as subsidies, special tax treatment, loans or revenue from government-mandated fees;

4. Whether the entity's key officers and directors are government officials or were appointed by government officials, and whether the Russian government has the power to fire the officers or directors of the entity;

58. Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 60:2–10.
59. United States v. Esquenazi, 752 F.3d 912, 920–33 (11th Cir. 2014).
60. *Id.* at 925.
61. *Id.* at 925–26; FCPA Resource Guide, *supra* note 2, at 20.
62. *See, e.g.*, Transcript, *Lambert*, No. 18-cr-12, ECF No. 152*;* Transcript, United States v. Pierucci, No. 12-cr-238 (D. Conn. Nov. 6, 2019), No. ECF 601; Orders, *Carson*, No. 09-cr-77, ECF Nos. 373, 549; United States v. Aguilar, 783 F. Supp. 2d 1108, 1115 (C.D. Cal. 2011).
63. Order at 2, *Lambert*, No. 18-cr-12, ECF No. 29.

5. The degree to which the entity's profits, if any, go directly into the government's treasury and the extent to which the government funds the entity if it fails to break even;

6. TENEX and TENAM's obligations and privileges under Russian law including whether TENEX and TENAM exercise exclusive or controlling power to administer their functions; and

7. The length of time these indicia have existed.[64]

Function

1. Whether TENEX or TENAM has a monopoly over the functions it exists to carry out;

2. Whether the government subsidizes the costs associated with the entity providing services;

3. Whether the entity provides services to the public at large in the foreign country;

4. Whether the public and the government of the foreign country generally perceive the entity to be performing a government function.[65]

The court made clear that the factors are not exhaustive and that no single factor would determine whether the relevant entity is an instrumentality of the foreign government.[66] Prosecutors should make sure the court also makes clear in its instructions, as it did in *Lambert*, that the jury need not find that all the factors listed above weigh in favor of an entity being an instrumentality.[67] The jury should understand that if it finds that the entity is an instrumentality, it must find that its employees (or anyone acting in an official capacity for or on behalf of that instrumentality) are "foreign officials" for purposes of the FCPA.[68]

In elucidating and applying the *Esquenazi* factors, it can be helpful for the jury to hear from a witness with competent knowledge of the history and structure of the foreign government and its laws, or other relevant expertise, such as the sector in which the relevant instrumentality functions. For that reason, depending on the facts of the case, it may be helpful to offer expert testimony to establish this element. In *Lambert*, for example, the prosecution team called Anne Harrington, a former U.S. government official with a remarkable background in national security, arms control, and nuclear non proliferation matters.[69] She had also lived in and traveled regularly to Russia

64. Nov. 14 *Lambert* Trial Transcript, *supra* note 14, at 60–61.
65. *Id.* at 61.
66. *Id.* at 61–62.
67. *Id.* at 62:2–5.
68. *Id.* at 62; 15 U.S.C. § 78dd 2(h)(2)(A).
69. Oct. 30 Afternoon *Lambert* Trial Transcript, *supra* note 18, at 9:22–17:21.

and had direct dealings with ROSATOM's predecessor, the Ministry of Atomic Energy of the Russian Federation, until that organization's reincorporation as ROSATOM.[70.] Ms. Harrington was also directly involved in the Megatons to Megawatts Agreement.[71.]

As an expert, Ms. Harrington was able to provide compelling testimony, based on her first-hand experiences and knowledge of the Russian government, that TENEX and TENAM were instrumentalities under the FCPA.[72.] For example, she provided testimony that Russia has "always treated uranium as a national strategic asset,"[73.] that Russia has "never let uranium out of government control ever,"[74.] and that TENEX, TENAM, and ROSATOM were all "organizations . . . 100 percent controlled by the Russian government."[75.]

III. Conclusion

Successfully prosecuting an FCPA case requires judicious attention at both the investigative and trial stages. Prosecutors should take care not to focus myopically on the narrative that makes the bribery scheme compelling to a jury, despite the narrative often being the most interesting part of a case. For example, before getting too far down the road to indictment, they should take special care to ensure that the statute properly covers the defendants whom they expect to charge, and that the officials who were bribed properly qualify as "foreign officials" under the FCPA.

About the Authors

David I. Salem is a Senior Litigation Counsel in the Greenbelt office in the District of Maryland. In his more than three decades as a federal prosecutor, he has tried more than 50 federal felony cases, including complex white-collar cases such as *United States v. Mark Lambert*, and has prosecuted cases such as *United States v. Vadim Mikerin* and *United States v. Transport Logistics International, Inc.* He is an adjunct professor in the Criminal Justice Department of the University of Maryland and at Catholic University Law School in Washington, D.C. He has previously lectured on white-collar prosecutions in Ashgabat, Turkmenistan; Kiev, Ukraine; and Almaty, Kazakhstan. The successful FCPA prosecution of Mark Lambert was the first of its kind in the district. He received his B.A. in Russian from the State University of New York at Albany and his J.D.–M.B.A. from the University of Maryland.

Derek J. Ettinger is an Assistant Chief in the FCPA Unit of the Criminal Division's Fraud Section. In his more than seven years in the FCPA Unit, he has prosecuted a range of corporate and individual cases, including

70. *Id.* at 17:17–18:10.
71. *Id.* at 10:1–16.
72. *Id.*
73. *Id.* at 61:24–25.
74. *Id.* at 62:6–7.
75. *Id.* at 63:2–3.

United States v. Mark Lambert, *United States v. Vadim Mikerin*, and *United States. v. Transport Logistics International, Inc.* Derek received his B.A. from the University of Arizona, his M.A. and Ph.D. in Philosophy from Brown University, and his J.D. from Columbia Law School. Before joining the Fraud Section, he served as Special Counsel to the Moreland Commission to Investigate Public Corruption.

Page Intentionally Left Blank

Federal Prosecution of Elder Financial Abuse: Combatting Power-of-Attorney Fraud

Timothy L. Vavricek
Assistant United States Attorney
United States Attorney's Office
Northern District of Iowa

> *"Our society must make it right and possible for old people not to fear the young or be deserted by them, for the test of a civilization is the way that it cares for its helpless members."*
>
> — Pearl S. Buck, The Good Earth

I. Introduction

Elder financial abuse is a rampant and growing problem throughout the United States, and the Department of Justice (Department) is committed to fighting it.[1] One of the more pernicious means by which fraudsters victimize the elderly is the familiar and ubiquitous legal instrument known as the "power of attorney." When a power of attorney is used in a fraud scheme against an elder, however, there is an unfortunate tendency among some prosecutors and law enforcement officers to view the fraud as only a civil matter, such as a breach of fiduciary duty under state law. But the Department has prosecuted power-of-attorney fraud successfully in district courts across the country.[2] This article discusses pathways and provides guidance for the successful federal prosecution of power-of-attorney fraud in elder financial abuse cases, including considerations under the United States Sentencing Guidelines (Guidelines).

---

1. The Elder Justice Initiative's website demonstrates the Department's commitment to combatting elder fraud and abuse and was an invaluable resource for writing this article. *See generally Elder Justice Initiative (EJI)*, U.S. Dep't of Just., https://www.justice.gov/elderjustice (last visited Oct. 3, 2022).
2. *See*, *e.g.*, Press Release, U.S. Dep't of Just., Burlington County Man Sentenced to 42 Months in Prison for Role in $350,000 Fraud Scheme (Dec. 9, 2021); Press Release, U.S. Dep't of Just., Raeford Certified Nursing Assistant Sentenced for Elder Fraud (Oct. 15, 2021); Press Release, U.S. Dep't of Just., Former Waterloo Medicaid Provider Sentenced to More than Five Years in Federal Prison for Defrauding Elderly Victim (June 28, 2021); Press Release, U.S. Dep't of Just., Lincoln Man Sentenced for Stealing Funds From His Elderly Father (Aug. 19, 2019).

II. The problem

A. Elder financial abuse

Elder financial abuse is a form of abuse by which the elderly, who are typically defined as someone at least 60 or 65 years old,[3] are exploited for financial gain.[4] As state legislatures have recognized, elder financial abuse may take many forms, including fraud, deception, intimidation, undue influence, and countless other means of obtaining money and property from an elderly person.[5]

The available sociological literature is remarkably devoid of statistical analyses of the incidence of elder financial abuse and its costs to our country.[6] Elder abuse is often characterized as a "hidden" problem because the extent and cost of crime perpetrated against the elderly has proven difficult to calculate.[7] The causes of this opacity include "underreporting, lack of reliable national data collection methods, and research study limitations."[8] This paucity of information is particularly true in the criminal justice system, where "justice system data on elder abuse are incomplete and unreliable."[9]

The available estimates of the scope and cost of elder financial abuse are "staggering" and "vary widely."[10] Studies have estimated that as many as one in five Americans over the age of 65 is a victim of elder financial abuse at an annual cost of anywhere between $3 billion and $36 billion.[11] Due to embarrassment, fear, intimidation, and incapacity, one study found that perhaps as

---

3. *See* Jesse R. Morton & Scott Rosenbaum, *An Analysis of Elder Financial Exploitation: Financial Institutions Shirking Their Legal Obligations to Prevent, Detect, and Report This "Hidden" Crime*, 27 Elder L.J. 261, 265–66 (2019). The Department defines an "elder" as someone 60 years or older. Elder Abuse Prevention and Prosecution Act (EAPPA), Pub. L. 115-70, § 2, 131 Stat. 1208, 1208 (2017) (adopting definition at 42 U.S.C. § 1397j(5)).

4. *See* Shelly L. Jackson & Thomas L. Hafemeister, Nat'l Inst. of Just., Financial Abuse of Elderly People vs. Other Forms of Elder Abuse 24–26 (2010).

5. *See*, *e.g.*, Del. Code Ann. tit. 31, § 3902(12) (2018) (defining "financial exploitation" in civil context); Vt. Stat. Ann. tit. 33, § 6902(6) (2021) (similar).

6. *See* Thomas L. Hafemeister, *Financial Abuse of the Elderly in Domestic Settings*, *in* Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America 382, 382–83 (Richard J. Bonnie & Robert B. Wallace eds., Nat'l Acads. Press 2003) ("Little empirical research has been conducted that directly addresses financial abuse of the elderly, and in general it has received less attention than other forms of elder abuse. . . . [M]ost commentary rests on a relatively thin empirical base and draws heavily on anecdotal observations . . . .").

7. *Id.* at 389; Brenda K. Uekert & Richard Van Duizend, *Resources for Fighting Elder Abuse—The Hidden Crime*, 24 Experience, no. 1, 2014, at 26.

8. Uekert & Van Duizend, *supra* note 7, at 26.

9. *Id.* at 27.

10. Morton & Rosenbaum, *supra* note 3, at 273.

11. *Id.* at 274.

few as 1 in 44 cases of elder financial abuse are reported to authorities.[12]

B. The power of attorney

Based on this author's experience, one of the primary and most devastating means by which fraudsters commit elder financial abuse is through a legal instrument known as the power of attorney. This situation is especially true when the perpetrator of elder financial abuse is a family member or acquaintance, which is often the case.[13]

A power of attorney is generally defined as "[a]n instrument in writing whereby one person, as principal, appoints another as [the principal's] agent and confers authority to perform certain specified acts or kinds of acts on behalf of [the] principal."[14] In many jurisdictions, the agent is referred to as the principal's "attorney in fact."[15] A power of attorney may be "durable," that is, remain in effect notwithstanding the principal's subsequent incapacity or other disability.[16] A power of attorney creates a fiduciary relationship between the principal and the attorney in fact or agent under state agency law.[17]

By design, the power of attorney is a private, contractual, and largely unregulated financial planning and management tool.[18] With a broadly worded power of attorney, it is possible for the agent to obtain complete and total access to an elder's finances, including signatory authority, without oversight from third-party trustees or the government. Presenting the power of attorney to a financial institution as prima facie evidence of the agent's right to control the principal's assets, the agent may gain access to the principal's checking

---

12. *Id.* (citing Consumer Reports study).
13. Hafemeister, *supra* note 6, at 384, 389.
14. *Power of Attorney*, Black's Law Dictionary (6th ed. 1991) (citing Complaint of Bankers Tr. Co. v. Bethlehem Steel Corp., 752 F.2d 874, 881 (3d Cir. 1984)).
15. Comm'n on L. & Aging, Am. Bar Ass'n, Selected Issues in Power of Attorney Law (2020) (chart detailing various state laws regarding powers of attorney); *see*, *e.g.*, Kindred Nursing Ctrs. Ltd. P'ship v. Clark, 137 S. Ct. 1421, 1425 (2017) ("At all times relevant to this case, [Respondents] each held a power of attorney, designating her as an 'attorney-in-fact' . . . and affording her broad authority to manage her family member's affairs.").
16. *Power of Attorney*, Black's Law Dictionary (11th ed. 2019). Durable powers of attorney were unknown at common law; Virginia enacted the first durable power-of-attorney statute in 1954. *See* Carolyn L. Dessin, *Acting as Agent Under a Financial Durable Power of Attorney: An Unscripted Role*, 75 Neb. L. Rev. 574, 577–80 (2015) (outlining evolution of durable powers of attorneys and noting that all fifty states and the District of Columbia have now enacted durable power-of-attorney statutes).
17. *See*, *e.g.*, Schock v. Nash, 732 A.2d 217, 224–25 (Del. 1999).
18. *See* Linda S. Whitton, *The Uniform Power of Attorney Act: Striking A Balance Between Autonomy and Protection*, 1 Phoenix L. Rev. 343, 345 (2008) ("In theory, a durable power of attorney is a far more flexible mechanism for surrogate property management than either a guardianship or a trust. Unlike a guardianship, where both the extent of the protected person's property and the guardian's actions are subject to court scrutiny, the power of attorney is a private arrangement between the principal and the agent.").

and savings accounts, retirement funds, annuities, and cash-value life insurance policies, for example. The power of attorney may also grant the agent unfettered ability to dispose of the agent's real and personal property.

The dangers of self-dealing are well-known, particularly in durable powers of attorney and principals suffering from an incapacity.[19] Self dealing, especially when committed under the guise of a legitimate transaction for the benefit of the principal, "is particularly difficult to prevent because the agent is using a valid power of attorney with sufficient authority for the underlying transaction."[20] The general response in the civil law to guard against self-dealing consists of default state law provisions that require the agent to "act loyally for the principal's benefit[,]" avoid conflicts of interest, and maintain records.[21] Owing to its contractual nature, however, the terms of the power of attorney may override many of these default duties and conceal the agent's actions from third parties absent a court order for disclosure.[22] By ensuring that the power of attorney is broadly worded and stripped of provisions that protect the principal, the agent may weaponize the power against the principal and cloak the agent's self-dealing under the guise of acting on the written authority of the principal.

III. Prosecuting elder financial abuse

State legislatures across the nation have enacted legislation to combat elder financial abuse.[23] Effective July 1, 2022, the state of Iowa became the last state to criminalize elder abuse.[24] Although the U.S. Code presently lacks a federal

19. *Id.* at 357.
20. *Id.* at 358.
21. *See* Linda S. Whitton, *Navigating the Uniform Power of Attorney Act*, 3 Nat'l Acad. Elder L. Att'ys J. 1, 16 (2007).
22. *See* Unif. Power of Att'y Act § 114 (Nat'l Conf. of Comm'rs on Unif. State L. 2006) [hereinafter UPOAA] (prefacing duties with the proviso "[n]otwithstanding provisions in the power of attorney"); *id.* § 114(h) cmt. ("The narrow categories of persons that may request an agent to account are consistent with the premise that a principal with capacity should control to whom the details of financial transactions are disclosed.").
23. Heather Morton, *Combatting Elder Financial Exploitation*, Nat'l Conf. of State Legislatures: LegisBriefs (May 2018), https://www.ncsl.org/research/financial-services-and-commerce/combatting-elder-financial-exploitation.aspx (stating that as of 2018, "[t]he number of bills introduced by state legislators to combat elder financial exploitation increased by more than 57% in three years" and "[i]n 41 states, the District of Columbia[,] and the U.S. Virgin Islands, lawmakers have enacted tougher criminal penalties to combat financial exploitation of older people and vulnerable adults").
24. Tom Barton, *Iowa Becomes Last State to Criminalize Elder Abuse: Reynolds Signs Law That Advocates Have Pressed for Years*, Gazette (Cedar Rapids) (June 15, 2022),
https://www.thegazette.com/government-politics/iowa-becomes-last-state-to-criminalize-elder-abuse/; *see* Iowa Code §§ 708.2D, 714.2A(2022) (providing enhanced penalties for crimes of assault and theft committed against persons

criminal statute that specifically targets and punishes the widespread problem of elder financial abuse, there is a stated congressional sense that elder abuse is an "affront to America's older adults" and that "we must do everything possible to both support victims of elder abuse and prevent the abuse from occurring in the first place."[25] Federal prosecutors, therefore, should use the familiar tools of fraud prosecutions when a power of attorney is used to commit elder financial abuse.

According to the National Center on Elder Abuse, when a power of attorney is used to commit elder financial abuse, victims and their family members often indicate that "their attempts to report this abuse to law enforcement are rebuffed with the following statement: 'It's a civil problem. Go talk to a civil lawyer.'"[26] This prevailing attitude accords with the author's experience. While the civil law may provide an available, if expensive, time-consuming, and ultimately ineffectual, remedy for elder financial abuse, it is not an exclusive remedy. In appropriate cases, an agent who uses the power of attorney as a "license to steal" may merit criminal prosecution.[27]

As indicated above, many state laws specifically target elder financial abuse. State authorities may bring charges under those statutes or, by further applying their police powers, under more general statutory provisions against theft and embezzlement, for example.[28] But what, if anything, may federal prosecutors do when an agent uses a power of attorney for self-dealing with fraudulent intent? As is often the case where there are vexing fraud schemes that threaten the national welfare, the answer lies in the mail, wire, and bank fraud statutes, 18 U.S.C. §§ 1341, 1343, and 1344, respectively.

The federal mail, wire, and bank fraud statutes[29] remain the most important "stopgap devices" available to the federal prosecutor, unless Congress

---

criminalizing assault against persons 60 years of age and older).

25. EAPPA § 301. The EAPPA estimates that "[n]ot less than $2,900,000,000 is taken from older adults each year due to financial abuse and exploitation." *Id.* The EAPPA provides for increased statutory maximum sentences for email and telemarketing scams targeting persons over the age of 55. 18 U.S.C. § 2326(2)(B). This sentencing provision of the EAPPA, however, has and will likely continue to have little effect given that (1) the statute only applies to telemarketing and email marketing and (2) very few offenders are sentenced at the statutory maximum violating 18 U.S.C. §§ 1341 (20 years), 1343 (20 years), and 1344 (30 years).

26. Lori A. Stiegel, Am. Bar Ass'n, Durable Power of Attorney Abuse: It's a Crime Too 1 (2008).

27. *See id.* at 2.

28. *See* Oklahoma v. Castro-Huerta, 142 S. Ct. 2486, 2502–03 (2022); Torres v. Lynch, 578 U.S. 452, 458 (2016).

29. 18 U.S.C. §§ 1341, 1343, 1344. In addition to the so-called "direct" theories of mail, wire, and bank fraud discussed in this article, some courts had approved prosecuting power-of-attorney self dealing on an honest services theory under 18 U.S.C. § 1346. *See, e.g.,* United States v. Williams, 441 F.3d 716, 722–24 (9th Cir. 2006). The honest services avenue appears closed after Skilling v. United States, 130 S. Ct. 2896, 2932 (2010), which held that section 1346 applies only to "bribery and kickback" schemes and not to "undisclosed self-dealing by a public official or private employee."

enacts a federal elder financial abuse statute.[30]

The mail fraud statute (18 U.S.C. § 1341) criminalizes the execution of any scheme to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, involving a mailing. Then-Assistant United States Attorney Jed Rakoff, later Judge Rakoff, famously referred to the mail fraud statute as "our Stradivarius" and "true love."[31]

The wire fraud statute (18 U.S.C. § 1343) is similarly "broad in scope" and criminalizes executing such schemes "to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises" if a wire transmission passes in interstate commerce.[32] In our modern, interconnected world, such interstate wire transmissions are abundant and include cell phone calls,[33] email,[34] and the ACH transactions that underlie most check deposits.[35]

The bank fraud statute (18 U.S.C. § 1344) should not be forgotten when, as is often the case, the elder's funds were under the custody or control of a federally insured financial institution,[36] such as a bank or credit union. In two relatively recent cases, *Loughrin v. United States*[37] and *Shaw v. United States*,[38] the Supreme Court has made clear that the bank fraud statute is not limited to schemes in which the financial institution is itself the intended target of the crime. In *Loughrin*, the Supreme Court held that intent to defraud a bank is not necessary to prove bank fraud and upheld applying the bank fraud statute to a scheme in which the defendant made false statements, in the form of forged and altered checks, to a merchant that the merchant would forward to a bank for payment in the ordinary course of business.[39] In *Shaw*, the Supreme Court held "a scheme fraudulently to obtain funds from a bank depositor's account normally is also a scheme fraudulently to obtain property from a 'financial institution.'"[40]

In cases wherein the principles of federal prosecution are otherwise sat-

---

30. *See* United States v. Maze, 414 U.S. 395, 405–06 (1974) (Burger, C.J., dissenting) ("Section 1341 of Title 18 U.S.C. has traditionally been used against fraudulent activity as a first line of defense. When a 'new' fraud develops—as constantly happens—the mail fraud statute becomes a stopgap device to deal on a temporary basis with the new phenomenon, until particularized legislation can be developed and passed to deal directly with the evil.").
31. Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 Duquesne L. Rev. 771, 771 (1980).
32. 18 U.S.C. § 1343; *see also* United States v. Gilbertson, 970 F.3d 939, 947 (8th Cir. 2020).
33. *See, e.g.*, United States v. Radomski, 473 F.3d 728, 729–30 (7th Cir. 2007).
34. *See, e.g.*, United States v. Hoffman, 901 F.3d 523, 546–47 (5th Cir. 2018).
35. *See, e.g.*, United States v. Zander, 794 F.3d 1220, 1231 (10th Cir. 2015).
36. *See* 18 U.S.C. § 20 (defining "financial institution").
37. 573 U.S. 351 (2014).
38. 580 U.S. 63 (2016).
39. *Loughrin*, 573 U.S. at 353, 364–65 (construing 18 U.S.C. § 1344(2)).
40. *Shaw*, 580 U.S. at 67 (construing 18 U.S.C. § 1344(1)).

isfied,[41] the putative defendant's possession of a power of attorney over the elderly victim's finances is no shield to federal prosecution; to the contrary, both the creation and the use of the power of attorney may be strong evidence that mail, wire, or bank fraud was committed to perpetuate elder financial abuse.

A. Fraud in creating the power of attorney

In some cases, the power of attorney is itself the product of fraud. The paradigm case involves the fraudster who creates a power of attorney by means of forging the principal's signature. In these cases, the prosecutor should proceed on the theory that the power of attorney is itself an instrumentality and evidence of the fraud, much like any other false or forged document.[42] Prosecution under the aggravated identity theft statute
(18 U.S.C. § 1028A) may be appropriate in these more straightforward cases. Interviews of the principal, the agent, and any purported witnesses to the signing of the power of attorney, such as a notary official, may be appropriate to establish that the power of attorney is a forgery.

More commonly, however, the agent takes advantage of the elder's mental incapacity or physical ailments and convinces the elder to sign a power of attorney without the elder understanding its import. In these cases, the prosecutor should attack the validity of the power of attorney as void or voidable.[43] Again, the prosecutor may argue that the power of attorney was obtained through fraud in the inducement, and thus is an instrumentality and evidence of the fraud. In addition to interviewing the principal, the agent, and any witnesses to the signing of the power of attorney, investigators should gather evidence, such as medical records, to establish not only the principal's incapacity to contract but also whether the agent knew of that incapacity.[44]

In some cases, a lawyer will have drafted or otherwise assisted in procuring the power of attorney. In these cases, the prosecutor should carefully analyze whether the attorney's client was the principal or the agent.[45] If the lawyer

41. Justice Manual 9-27.001–9-27.760.
42. *See* United States v. Louper-Morris, 672 F.3d 539, 556–57 (8th Cir. 2012).
43. Nearly 150 years ago, the Supreme Court held that, as a matter of federal law, "a power of attorney executed by an insane person, or one of unsound mind, is absolutely void." Dexter v. Hall, 82 U.S. 9, 12 (1872). The present majority rule among the states is that mental incompetence merely renders written agreements voidable, not void. 5 Richard A. Lord, Williston on Contracts § 10:3 (4th ed. 2022) ("The vast majority of courts more commonly express the view that an incompetent person's transactions are voidable.").
44. Nursing home records may provide a wealth of information in this regard. For example, nursing homes routinely gauge the mental acuity of their residents through administering a so-called Brief Interview for Mental Status (BIMS) test and log visitors to their facilities.
45. Although tracing payment for the attorney's fees may help to provide the answer to this question, it is not dispositive. *See* Model Rules of Pro. Conduct r. 5.4(c) (Am. Bar Ass'n 1983) (contemplating third-party payment for legal fees so long as the lawyer does not permit that third party "to direct or regulate the lawyer's

represented the agent, then it may be appropriate to interview or otherwise obtain evidence from the lawyer about the circumstances surrounding the signing of the power of attorney, much like any other witness. Care should be taken, however, to comply with Justice Manual 9-13.410 (Guidelines for Issuing Subpoenas to Attorneys for Information Relating to the Representation of Clients). If the lawyer represented the principal, conflict-of-interest concerns may arise that may dissuade the lawyer from cooperating in the investigation even though cooperation ordinarily would be in the principal's best interests when the agent is using the power of attorney to exploit the principal financially.[46]

B. Fraud in using the power of attorney

The agent's use of the power of attorney may also provide strong evidence of fraud. At the outset, the prosecutor should carefully examine the provisions of the power of attorney to determine whether the agent has violated its terms. As indicated in Section II.A above, many default state law provisions (reflected in a model "bar form," for example) prohibit self-dealing and require the agent to act loyally for the principal's benefit, avoid conflicts of interest, and maintain records.[47] If, for example, the power of attorney at issue forbids the agent from making gifts or other transfers to the agent, and the investigation reveals that the agent routinely authorized wire transfers from the principal's financial accounts to the agent's own accounts, then both the power of attorney and the wire transfers may provide intrinsic evidence of a wire fraud scheme.

For example, in *United States v. Thomas*, the defendants were convicted at trial of wire fraud and conspiracy to commit mail and wire fraud in conjunction with their operating a loan brokerage firm.[48] On appeal, the Eleventh Circuit Court of Appeals observed that "the most compelling witness for the prosecution" was a military officer who had granted one of the defendants a power of

professional judgment in rendering such legal services").

46. The Model Rules of Professional Conduct (Model Rules) state, "When a client's capacity to make adequately considered decisions in connection with a representation is diminished, whether because of minority, mental impairment or for some other reason, the lawyer shall, as far as reasonably possible, maintain a normal client-lawyer relationship with the client." *Id.* at r. 1.14(a). The Model Rules, however, authorize the lawyer to take protective action if "the client has diminished capacity, is at risk of substantial . . . financial . . . harm unless action is taken and cannot adequately act in the client's own interest." *Id.* at r. 1.14(b). The commentary to the Model Rules states that "[t]he normal client-lawyer relationship is based on the assumption that the client, when properly advised and assisted, is capable of making decisions about important matters." *Id.* at r. 1.14 cmt 1. The commentary attempts to distinguish between the "severely incapacitated person" who "may have no power to make legally binding decisions" and "a client with diminished capacity" who "often has the ability to understand, deliberate upon, and reach conclusions about matters affecting the client's own well-being." *Id.* It is unclear whether the legal profession is trained to make these distinctions and, if not, what steps a lawyer should take to ascertain in which category the client falls.

47. Whitton, *supra* note 18, at 3, 16 (citing UPOAA § 114).

48. United States v. Thomas, 62 F.3d 1332, 1335 (11th Cir. 1995).

attorney.[49] The defendants misused the power of attorney to borrow money without the officer's knowledge and failed to repay the loan.[50] The Eleventh Circuit held that evidence of the defendants' misuse of the power of attorney was intrinsic to the charged federal fraud offenses.[51] Even though the defendants "were not indicted for their actions in borrowing money in [the officer's] name without informing him, and without transferring the proceeds to him[,]" the court found his testimony admissible because "those actions arose out of a fraudulent activity with which the [defendants] *were* charged—namely, devising a scheme to fraudulently obtain money from individuals and businesses who were interested in receiving substantial loans."[52]

Once the prosecutor establishes that the agent used the power of attorney for the agent's own benefit, inconsistently with the terms of the power of attorney, an inference of fraud arises. Historically, state agency law so frowns upon an agent's self-dealing that courts have characterized transactions for the agent's own benefit under a power of attorney as "prima facie evidence" of fraud, shifting the burden to the agent to prove that such transactions were not fraudulent. One state Supreme Court recently summarized these principles of agency law as follows:

> A cause of action for fraud . . . exists . . . in the context of self-dealing through the use of a power of attorney. We have held:
>
> > [A] prima facie case of fraud is established if the plaintiff shows that the defendant held the principal's power of attorney and that the defendant, using the power of attorney, made a gift to himself or herself. . . . The burden of going forward under such circumstances falls upon the defendant to establish by clear and convincing evidence that the transaction was made pursuant to power expressly granted in the power of attorney document and made pursuant to the clear intent of the donor.
>
> Thus, once it is shown that the defendant used the power of attorney to make a gift to himself or herself, the burden is upon the defendant to establish by clear and convincing evidence that the transaction was made with the clear intent of the donor.[53]

49. *Id.* at 1342.
50. *Id.*
51. *Id.*
52. *Id.*
53. Litherland v. Jurgens, 869 N.W.2d 92, 97–98 (Neb. 2015) (quoting Crosby v. Luehrs, 669 N.W.2d 635, 645 (Neb. 2003)); *see also* 37 George Blum et al., American Jurisprudence: Fraud and Deceit § 461 (2d ed. 2022) (observing that "a presumption of fraud arises where there is an indication of fraud or self-dealing by the fiduciary . . . where a duty under the fiduciary or confidential relationship has been abused or breached or where the superior party or fiduciary profits or obtains a possible benefit from the relationship[,] [or] when property is transferred between a fiduciary and his or her principal" and collecting cases (footnotes omitted)).

While the defendant in a criminal prosecution bears no burden, of course, the foregoing cases make clear that self-dealing under a power of attorney is not a mere breach of fiduciary duty. Self-dealing may give rise to an inference of fraud. While the prosecutor bears a heavier burden to prove criminal intent beyond a reasonable doubt than the plaintiff in a civil fraud action,[54] the same principles that support *de jure* inference of civil fraud also should give rise to *de facto* inferences of criminal fraud in prosecutions for elder financial abuse.

C. Sentencing considerations, including restitution

Perpetrators of elder financial abuse face potentially significant penalties under the mail, wire, and bank fraud statutes. The statutory maximum sentence for each count of mail and wire fraud is 20 years with a 3-year term of supervised release.[55] The maximum sentence for each count of bank fraud is 30 years with a 5-year term of supervised release.[56] Probation is not authorized upon conviction of bank fraud.[57]

Most defendants, of course, will not receive sentences anywhere near the maximum statutory sentence. The relevant sentencing factors are set forth in 18 U.S.C. § 3553(a) and include "the nature and circumstances of the offense and the history and characteristics of the defendant";[58] the need for the sentence "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment";[59] the need "to afford adequate deterrence to criminal conduct[,] to protect the public from further crimes of the defendant[,]" and to provide defendant with needed correctional treatment;[60] the defendant's guidelines range and the policy statements of the Sentencing Commission;[61] "the need to avoid unwarranted sentence disparities";[62] and "the need to provide restitution to any victims of the offense."[63]

The Guidelines provide for several enhancements that ordinarily will apply in elder financial abuse cases where the defendant utilizes a power of attorney to commit the fraud.[64] Applying these enhancements should result in a sentence of imprisonment even if the defendant lacks any criminal history.

Section 2B1.1 of the Guidelines applies in mail, wire, and bank fraud cases and carries a base offense level of seven.[65] If the loss to the victim of elder financial abuse exceeds $6,500, then a graduated, multi-level enhancement from

54. *See* Helvering v. Mitchell, 303 U.S. 391, 397–98 (1938).
55. 18 U.S.C. §§ 1341, 1343, 3581, 3583(b)(2).
56. 18 U.S.C. §§ 1344, 3581, 3583(b)(1).
57. *See* 18 U.S.C. § 3561.
58. 18 U.S.C. § 3553(a)(1).
59. *Id.* § 3553(a)(2)(A).
60. *Id.* § 3553(a)(2)(B)–(D).
61. *Id.* § 3553(a)(4)–(5).
62. *Id.* § 3553(a)(6).
63. *Id.* § 3553(a)(7).
64. *See generally* U.S. Sent'g Guidelines Manual (U.S. Sent'g Comm'n 2021) [hereinafter U.S.S.G.].
65. U.S.S.G. §§ 2B1.1(a)(1), app. A.

the loss table at section 2B1.1(b)(1) will apply.[66]

Three potential enhancements under the Guidelines may apply in cases in which a power of attorney is used to perpetrate elder financial abuse. First, a two-level enhancement applies if a victim of the crime suffered a substantial financial hardship.[67] The commentary to section 2B1.1 sets forth a list of non-exhaustive factors to determine whether the offense resulted in a substantial financial hardship.[68] These factors include "suffering substantial loss of a retirement, education, or other savings or investment fund"; "postponing . . . retirement plans"; and "making substantial changes to his or her living arrangements, such as relocating to a less expensive home."[69]

It is the author's experience that the substantial financial hardship enhancement ordinarily will apply when a power of attorney is used to perpetuate elder financial abuse. In the hands of a criminal, the power of attorney allows the perpetrator immediate access to all of the victim's financial accounts; the defendant may quickly drain a lifetime of savings and wealth in a matter of days. The attendant sudden loss of all of an elderly person's assets will have a devasting financial impact upon the elder with little to no prospect of recoupment in the elder's lifetime. The elder may be forced to leave a nursing home or assisted living facility in favor of a lower-cost option, a situation that should qualify the defendant for the enhancement.[70]

---

66. *See* U.S.S.G. § 2B1.1(b)(1) (providing for a 2-level increase if the loss exceeds $6,500, 4-level increase if greater than $15,000, 6-level increase if greater than $40,000, 8-level increase if greater than $95,000, 10-level increase if greater than $150,000, 12-level increase if greater than $250,000, 14-level increase if greater than $550,000, 16-level increase if greater than $1.5 million, and so on).

67. U.S.S.G. § 2B1.1(b)(2)(A)(iii); *see also* U.S. Sent'g Comm'n, Amendments to the Sentencing Guidelines 24 (2015) ("Consistent with the Commission's overall goal of focusing more on victim harm, the revised victims table ensures that an offense that results in even one victim suffering substantial financial harm receives increased punishment . . . .").

68. *See* U.S.S.G. § 2B1.1 cmt. n.4(F).

69. U.S.S.G. § 2B1.1 cmt. n.4(F)(iii)–(v).

70. *See*, *e.g.*, United States v. Kitts, 27 F.4th 777, 790–91 (1st Cir. 2022) (holding that the victim's "loss of her savings and the liquidation of her apartment, inescapably constitutes substantial financial hardship within the ambit of the guidelines"). In one case the author prosecuted, the victim was not only forced to leave her nursing home, but then had to move in with relatives that had perpetrated the elder financial abuse. The focus on substantial financial hardship, however, ignores the mental pain and anguish that the elder suffers. The Guidelines suggest that an upward departure may be appropriate if "[t]he offense caused or risked substantial non-monetary harm[,]" such as "physical harm, psychological harm, or severe emotional trauma." U.S.S.G. § 2B1.1 cmt. n.21(A)(ii). Needless to say, losing one's life savings may cause psychological harm or severe emotional trauma, and to the extent that one must move, "transfer trauma" is a known physical risk to the elder. *See*, *e.g.*, Terri D. Keville, *Studies of Transfer Trauma in Nursing Home Patients: How the Legal System Has Failed to See the Whole Picture*, 3 Health Matrix 421, 458 (1993) (concluding that advocates for the elderly should recognize that, while well-planned moves to superior facilities may enhance the elder's quality of life, "poorly planned and executed involuntary moves

Second, a two-level increase applies "[i]f the defendant knew or should have known that a victim of the offense was a vulnerable victim."[71] The Seventh Circuit Court of Appeals has observed that elderly victims frequently will qualify as vulnerable victims under the Guidelines, "especially when their financial investments and financial security are at issue."[72] The Guidelines define a "vulnerable victim" to include someone "who is unusually vulnerable due to age, physical or mental condition, or who is otherwise particularly susceptible to the criminal conduct."[73] In cases involving a power of attorney, the knowledge requirement of section 3A1.1 ordinarily will be met because of the necessary contact between the principal and agent to obtain the power of attorney in the first place as well as the stated purposes of the power of attorney.[74]

Third, a two-level enhancement should apply for an abuse of private trust, under section 3B1.3, at least in cases in which the power of attorney was not itself an outright forged instrument. This Guideline applies if the defendant abused a position of private trust "in a manner that significantly facilitated the commission or concealment of the offense."[75] Courts have routinely applied this enhancement when the defendant used a power of attorney to commit the fraud offense,[76] and the result should be no different in cases of elder financial abuse.

Restitution to the elder abuse victim for the full amount of loss that the perpetrator caused in the scheme to defraud is mandatory upon conviction of the mail, wire, and bank fraud statutes.[77] If the elder abuse victim predeceases the restitution judgment, restitution must be made to the victim's estate.[78] If the perpetrator is a family member or other person who otherwise might inherit or receive benefits from the victim's estate, the prosecutor in consultation with the victim or the victim's guardian or executor may request that the district court include a provision in the restitution order to ensure that the perpetrator does not benefit from restitution.[79]

---

can be extremely harmful to elderly patients").

71. U.S.S.G. § 3A1.1(b)(1).

72. United States v. Iriri, 825 F.3d 351, 352 (7th Cir. 2016) (quoting United States v. Sims, 329 F.3d 937, 944 (7th Cir. 2003)).

73. U.S.S.G. § 3A1.1 cmt. n.2(B).

74. It is not double counting to apply the two-level substantial financial hardship and vulnerable victim enhancements. *See* U.S.S.G. § 2B1.1 cmt. n.4(D).

75. U.S.S.G. § 3B1.3.

76. *See, e.g.*, United States v. Fiorito, 640 F.3d 338, 351–52 (8th Cir. 2011); United States v. Johnson, 422 F. App'x 281, 282–83 (4th Cir. 2011) (unpublished).

77. 18 U.S.C. § 3663A(a)(2) (defining the victim and offense to include full restitution for scheme); *id.* § 3663A(c)(1)(A)(ii) (mandating restitution for "offense[s] against property . . . including any offense committed by fraud or deceit").

78. *Id.* § 3663A(a)(1). A defendant may not be named as the victim's representative for purposes of a mandatory restitution order. *Id.* § 3663A(a)(2).

79. *See id.* § 3663(b)(5) (granting district court discretion to order the defendant to "make restitution to a person or organization designated by the victim or the estate"); *id.* § 3664(g)(2) (authorizing victim to designate restitution award to the Crime Victims Fund).

IV. Conclusion

The financial exploitation of the elderly is not always just a "civil matter" but also may implicate the criminal law. The federal prosecutor has a role in combatting elder financial abuse, including frauds perpetrated by means of a power of attorney. The mail, wire, and bank fraud statutes provide an important "stopgap" until such time as Congress may pass national legislation criminalizing this national scourge. Elder financial abuse is an area "most deserving of federal attention"[80] given its widespread, deleterious effects on our nation. Federal prosecutors should continue to use the familiar tools of fraud prosecutions when a power of attorney is used to commit elder financial abuse.

About the Author

Timothy L. Vavricek is an Assistant United States Attorney in the Criminal Division of the U.S. Attorney's Office for the Northern District of Iowa. Before joining the U.S. Attorney's Office, he served as an Assistant Attorney General at the Iowa Attorney General's Office and clerked for three judges: the Honorable William Jay Riley, Chief Judge of United States Court of Appeals for the Eighth Circuit; the Honorable Linda R. Reade, Chief Judge of the United States District Court for the Northern District of Iowa; and the Honorable Michael J. Streit, Justice of the Iowa Supreme Court.

80. Justice Manual 9-27.230.

Page Intentionally Left Blank

The PCSF: A Global Presence for a Global Problem

Philip Andriole & Chris Maietta
Trial Attorneys
Antitrust Division
New York Office

On October 18, 2021, two Belgian executives entered the U.S. Embassy in Brussels, nestled next to the historic Parc du Bruxelles. The pair, flanked by agents from the Defense Criminal Investigative Service (DCIS) and U.S. Army Criminal Investigation Division (Army CID), settled into a conference room. Meanwhile, federal prosecutors in their makeshift home offices in New York flicked on their cameras, along with a smattering of defense attorneys around the country. Around 9:15 a.m. in Washington, D.C., U.S. District Court Judge Tanya S. Chutkan brought the parties, spread across the continents, to order and began plea hearings for the two executives, Robby Van Mele and Bart VerBeeck. The two admitted their roles in a conspiracy to rig bids on contracts to provide security services for U.S. Department of Defense (DOD) bases in Belgium. The "Security Services" investigation that led to these pleas was a milestone achievement for the Procurement Collusion Strike Force (PCSF) and announced the PCSF's ambition to go wherever there is collusion—be it markets in New York City, San Francisco, or halfway around the world.

Launched in 2019, the PCSF is an interagency strike force comprising federal prosecutors from the Antitrust Division of the Department of Justice (Department) and 22 U.S. Attorneys' Offices (USAOs), as well as law enforcement agents from seven national partner agencies: the Federal Bureau of Investigation (FBI), two Offices of Inspector General of the DOD (the DCIS and the Air Force Office of Special Investigations), Department of Homeland Security, Department of Justice, General Services Administration, and Postal Service. The PCSF's primary mission is to deter, detect, investigate, and prosecute public procurement collusion and fraud cases at all levels of government—federal, state, and local. The PCSF's emphasis is on bad actors—both companies and individuals located in the United States and internationally—who are involved in antitrust crimes (for example, bid rigging, price fixing, market allocations, and conspiracies or attempts to monopolize) that violate Title 15 U.S.C. §§ 1–2 (the Sherman Act)[1] and other serious crimes such as wire fraud and mail fraud

1. The Sherman Act of 1890, ch. 647, 26 Stat. 209 (1890) (codified as amended at 15 U.S.C. §§ 1–38) criminalizes bid rigging, price fixing, and market allocation. *Id.* §§ 1–2. The Supreme Court has construed the statute to prohibit certain horizontal agreements between competitors as per se unlawful, including price fixing and bid rigging agreements. *See* United States v. Socony-Vacuum Oil Co., 310 U.S. 150,

schemes, among other Title 18 offenses. Special focus is placed on schemes that target the federal procurement process for goods and services, as well as state and local contracts that receive federal funding.

This article discusses a recent case—the Security Services investigation—that involved a cross-section of prosecutors and U.S. law enforcement agents located around the world before describing the broader objectives and capabilities of the PCSF.[2] The case highlights the work of the PCSF and demonstrates that borders are not limits for prosecuting crimes that corrupt the procurement process.[3] If bad actors undermine or distort the process in which the government acquires goods or services, then the PCSF will use all available tools to hold them accountable.

I. The Security Services investigation

This part will describe the market for security services in Belgium within the broader procurement context, the conspiring government contractors, their conspiracy, and the PCSF's investigation.

Criminal antitrust cases are often named for their markets. For example, four major banks pleaded guilty and paid a $2.5 billion criminal fine for foreign exchange market manipulation in the Antitrust Division's "FX Market" investigation in 2015,[4] with a related trial conviction of an FX trader in 2019.[5] In addition, a high-profile former CEO was convicted and sentenced to 40 months in prison for fixing the prices of packaged seafood in the "Canned Tuna" investigation in 2019.[6] In 2020, a generic drug manufacturer entered into a deferred prosecution agreement and agreed to pay a $195 million criminal penalty—the highest ever for a domestic cartel—for its role in fixing prices, rigging bids, and allocating customers in the sale of generic drugs in the "Generic Drug"

---

218 (1940). "A horizontal conspiracy exists when the coconspirators are 'competitors at the same level of the market structure' rather than 'combinations of persons at different levels of the market structure, e.g., manufacturers and distributors, which are termed "vertical" restraints.'" United States v. Aiyer, 470 F. Supp. 3d. 383, 403 (S.D.N.Y. 2020). The Antitrust Division can also bring charges under section 2 of the Sherman Act for conspiracies or attempts to monopolize, among other things. *See* 15 U.S.C. § 2.

2. This article discusses only substantive facts available in public filings and press releases. *See, e.g.*, Information, United States v. G4S Secure Solutions NV, No. 21-cr-432 (D.D.C. June 25, 2021), ECF No. 1; Indictment, United States v. Seris Sec. NV, No. 21-cr-443 (D.D.C. June 29, 2021), ECF No. 1 [hereinafter Seris Indictment].

3. See *Procurement Collusion Strike Force*, U.S. Dep't of Just., https://www.justice.gov/procurement-collusion-strike-force (last visited Sept. 6, 2022), for the latest news, policies, and updates from the PCSF.

4. Press Release, U.S. Dep't of Just., Five Major Banks Agree to Parent-Level Guilty Pleas (May 20, 2015).

5. Press Release, U.S. Dep't of Just., Former Trader for Major Multinational Bank Convicted for Price Fixing and Bid Rigging in FX Market (Nov. 20, 2019).

6. Press Release, U.S. Dep't of Just., Former Bumble Bee CEO Sentenced to Prison for Fixing Prices of Canned Tuna (June 16, 2020).

investigation.[7]

Similarly, the Security Services moniker understates a complex, global case involving a complex, global market. Although the contracts at issue comprised a small part of the U.S. procurement budget in Belgium, they were critical to keeping U.S. foreign installations safe. A brief review of the variety of other procurements in Belgium illustrates the scope of the challenge that officials face in identifying and preventing procurement misconduct overseas.

A. The market

In 1832, the then-fledgling United States established diplomatic relations with Belgium following its declaration of independence from the Netherlands.[8] Currently, Belgium hosts three DOD installations: Kleine Brogel Air Base, U.S. Army Garrison (USAG) BENELUX Brussels, and USAG BENELUX-SHAPE/Chiev. Since 2002, Belgium has also hosted a North Atlantic Treaty Organization (NATO) strategic military command called the Supreme Headquarters Allied Powers Europe (SHAPE), located near the city of Mons in southern Belgium. SHAPE houses NATO's Communications and Information Agency, technology, and cyber experts.[9]

These three U.S. bases are a small part of the DOD's overseas operations. It maintains around 65 installations in 24 nations. For the 2021 fiscal year, the DOD was allocated $140.7 billion of its near $705 billion discretionary budget authority for procurement. Spending data reflects that $19.7 billion was designated for performance in foreign countries.[10]

Thanks to USAspending.gov, any internet user can review granular data on U.S. procurement spending. For the 2021 fiscal year, the DOD made over 675 prime awards with Belgium as the place of performance, totaling over $180 million.[11] This amount covered things from sophisticated equipment like the GAU-21 .50 Cal. Machine Gun System (approximately $2.9 million to FN Herstal SA)[12] to mundane base work like utility modernization at Chievres (approximately $12.9 million to BB Government Services SPRL).[13] Filtering

---

7. Press Release, U.S. Dep't of Just., Major Generic Pharmaceutical Co. Admits to Antitrust Crimes (Mar. 2, 2020).
8. *U.S. Relations with Belgium*, U.S. Dep't of State (May 25, 2022), http://www.state.gov/r/pa/ei/bgn/2874.htm.
9. *About Us*, NATO Commc'ns & Info. Agency, https://www.ncia.nato.int/about-us.html (last visited Sept. 6, 2022).
10. U.S. Dep't of Def., Agency Financial Report 20 (2021).
11. *See Federal Awards*, USASpending.gov, usaspending.gov/search/?hash=e68c6987de821b68e2d041efc4187460 (last visited Sept. 13, 2022) (Filter Time Period: FY 2021; Place of Performance: Belgium; Awarding Agency: Department of Defense).
12. *Contract Summary: Award ID N0001920F0618*, USASpending.gov, https://www.usaspending.gov/award/CONT_AWD_N0001920F0618_9700_N0001919D0016_9700 (last visited Sept. 6, 2022).
13. *Contract Summary: Award ID W912GB21C0035*, USASpending.gov, https://www.usaspending.gov/award/CONT_AWD_W912GB21C0035_9700_-NONE-_-NONE-

by the North American Industry Classification System codes for "Investigation and Security Services" reveals seven awards totaling around $21.3 million for the 2021 fiscal year.[14.]

These services are a fraction of the DOD's procurement spending by any measure. The Belgium contracts at issue, however, included providing individual guards, mobile monitoring of certain locations, and electronic surveillance.[15.] These services, while not mission-critical, were vital to ensuring the safety of the installations and those working there. To secure these services at the best price for the taxpayer, these contracts underwent a competitive market bidding process.

B. The alleged conspirators

Enter the alleged conspirators. In this case, the key players were three Belgian security services firms: Seris Security NV (Seris), G4S Secure Solutions (G4S), and a third, unindicted corporate co conspirator. The two indicted firms were both parts of large entities with global footprints: Seris and G4S Global. Seris had more than 40,000 employees and €663 million revenue in 2021,[16.] while G4S, an Allied Universal company, has a network of 800,000 employees and annual revenues of approximately $20 billion.[17.]

Seris and G4S competed with each other to win local security services contracts. In the last 10 fiscal years, Seris received 16 prime awards from the DOD totaling just under $59 million for guard services; all but one specified Belgium as the place of performance.[18.] G4S was also a regularly winning government contractor, receiving 46 DOD prime contracts in the same period worth approximately $11.8 million for logistics, security, and maintenance services at bases around the world.[19.]

These corporations, of course, act through agents. G4S allegedly acted through three executives: CEO Jean Paul Van Avermaet, director of sales

---

(last visited Sept. 6, 2022).

14. *Federal Awards*, USASpending.gov, usaspending.gov/search (last visited Sept. 21, 2022) (Filter Time Period: FY 2021; Place of Performance: Belgium; Awarding Agency: Department of Defense; NAICS Codes 561612 and 561621; IDs W912PA21P0011, HE125421F2107, W912PA21F0010, W912PA21F0003, W912PA21F0021, W912PA21F0074, and W912PA18P0006).

15. Seris Indictment, *supra* note 2, at 1.

16. *A French Group with an International Dimension*, Seris Grp., https://seris-group.com/en/french-group-international-dimension (last visited Sept. 6, 2022).

17. *Who We Are*, G4S Glob., https://www.g4s.com/who-we-are (last visited Sept. 6, 2022).

18. *Federal Awards*, USASpending.gov, https://www.usaspending.gov/search/?hash=4b4dbf85981f44ca7f93795032954b73 (last visited Sept. 6, 2022) (Filter Time Period: FY 2013–FY 2022; Awarding Agency: DOD; Recipient: Seris Security NV).

19. *Federal Awards*, USASpending.gov, https://www.usaspending.gov/search/?hash=67b122cfb62a435cfead208993a39f17 (last visited Sept. 9, 2022) (Filter Time Period: FY 2013–FY 2022; Awarding Agency: Department of Defense; Recipient: G4S).

Bart VerBeeck, and director of operations Robby Van Mele. Seris allegedly acted through two executives: CEO Danny Vandormael and director Peter Verpoort. All were Belgian nationals with at least a decade of experience in the security services industry. In 2020, all five were charged in the PCSF's first global investigation.

C. The alleged conspiracy

The indictment alleges that, on September 17, 2019, Jean Paul Van Avermaet, the CEO of G4S, met Danny Vandormael, the CEO of Seris, for breakfast at a hotel in Brussels.[20] It further alleges that the two were more than friendly rivals. They were co-conspirators working to rig their bids on DOD contracts in Belgium.[21] As other executives have since admitted in their guilty pleas, the scheme began a few months earlier in the spring of 2019.[22] The arrangement was much like a classic smoke-filled, back-room, bid-rigging conspiracy, along with some modern touches—the breakfast in a hotel lobby coupled with incriminating phone calls, emails, and encrypted messages. The goal was simple: win contracts and receive payments for their services at inflated, anti-competitive prices.

For instance, the indictment alleges that in March 2020, Danny Vandormael worked with a competitor to ensure the competitor's company would bid at an artificially high price that Vandormael suggested.[23] What was the competitor's incentive to lose? It was what Vandormael allegedly called the "vice versa": Seris had allegedly submitted a "comp bid" (short for a "complementary" bid, one that is intentionally non-competitive and submitted only to give the appearance of competition) for a prior contract, which the competitor won, and now the competitor should reciprocate.[24] The conspirators allegedly deployed this arrangement on numerous contracts; the largest contract affected was valued at $77.36 million.[25]

The alleged breakfast-in-Belgium agreement, and the ongoing scheme it perpetuated, was a classic example of a bid-rigging conspiracy, which is a felony under federal law. Since its creation in 1919, the Antitrust Division has prosecuted bid-rigging, price-fixing, and market-allocation conspiracies under section 1 of the Sherman Act, and the security services conspiracy is an example of the type of criminal conduct that the PCSF has pursued since its inception in 2019.[26]

---

20. Seris Indictment, *supra* note 2, at 5–6.
21. *Id.* at 4.
22. *See* Plea Agreement at 4–5, United States v. VerBeeck, No. 21-cr-574 (D.D.C. Oct. 18, 2021), ECF No. 9.
23. Seris Indictment, *supra* note 2, at 5–6.
24. *Id.*
25. Plea Agreement at 4, United States v. G4S Secure Solutions NV, No. 21-cr-432 (D.D.C. July 16, 2021), ECF No. 9.
26. *See* U.S. Dep't of Just., An Antitrust Primer for Federal Law Enforcement Personnel (2022)[hereinafter ATR Primer].

D. The investigation and COVID-19

In March 2020, the world and the ways we live and work rapidly changed. In the Antitrust Division's New York office, prosecutors and paralegals had already been planning to decamp from 26 Federal Plaza—the Jacob K. Javits Federal Building—for much-needed renovations. Prosecutors expected to spend a few months either working from home or from an awkward collection of shared desks on a different floor. Their absence would be much longer and more challenging. On March 11, 2020, the World Health Organization declared COVID-19 a pandemic.[27.] Two days later, President Trump declared a National Emergency, and the administration issued a ban on travel from Europe.[28.] Offices closed, servers overloaded, and working with a colleague a few office doors away, let alone on a different continent, presented a range of new complications. Amidst the worsening catastrophe, the security services team was ramping up its investigation into the bid rigging taking place across the globe.

International investigations pose challenges ranging from the mundane—coordinating time zones, translating documents, etc.—to thornier issues like extradition, mutual legal assistance, and extraterritorial jurisdiction. The timing of the security services investigation and the COVID-19 pandemic heightened these challenges. The team was unable to meet in person and travel to Belgium was out of the question. Fortunately, the PCSF was prepared.

The cross-governmental strike force had connections with Army CID and DOD-DCIS agents abroad and domestically. The PCSF quickly staffed a skilled team with both international agents working in Belgium and FBI partners stationed a few floors down from the Antitrust Division in 26 Fed. Throughout the next year, the team conducted numerous interviews while navigating their way through now-familiar tools like Zoom and pandemic-imposed challenges like rolling lockdowns. Shortly after the pandemic began, G4S had agreed to plead guilty and cooperate.[29.]

The investigation endured COVID surges, prolonged office renovations, and winter storms while delivering a steady output of guilty pleas and a four-defendant indictment. The team indicted Seris, two of its former executives, and one G4S former executive in June 2021. G4S pleaded guilty in July 2021, agreeing to pay a $15 million criminal fine. Two former G4S executives pleaded guilty in October 2021. It is a watershed case for the PCSF, but only the beginning of its efforts to police procurement crimes on the global stage.

---

27. Tedros Adhanom Ghebreyesus, Director-General, World Health Org., Opening Remarks at the Media Briefing on COVID-19, (Mar. 11, 2020).
28. Proclamation No. 9994, Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak, 85 Fed. Reg. 15,337 (Mar. 13, 2020).
29. Press Release, Dep't of Just., Belgian Security Services Firm Agrees to Plead Guilty to Criminal Antitrust Conspiracy Affecting Department of Defense Procurement (June 25, 2021).

II. The PCSF & public procurement crimes

The Security Services investigation was PCSF's first—but certainly not last—international criminal enforcement action. It demonstrates the abilities of the virtual strike force and its focus on ensuring the integrity of public procurement. This part will describe the PCSF and its goals, review the conduct that the PCSF looks to prosecute, highlight the PCSF's accomplishments in the three years since its inception, and preview the future of the strike force.

As the security services investigation demonstrates, government procurement contracts often involve a competitive bidding process. Prospective vendors compete against each other to provide the best combination of high-quality goods or services at the lowest price. Just like any other consumer, the government, as a buyer, wants to pay the lowest price without sacrificing quality. Competitive bidding means prospective vendors must act independently. The process is frustrated when bad actors collude behind the scenes and agree on any number of things: Who will win a contract, by how much, how to meet non-price elements of a bid solicitation, or simply who will and will not bid. When competitors decide to cheat instead of compete, the procurement process is corrupted, the government is defrauded, and taxpayers pay more.

The problem of procurement crime is significant. The federal government spends billions of dollars each year procuring a range of goods and services. For the 2020 fiscal year, the federal government expended more than $665 billion on contracts for goods and services, including expenditures on roads, bridges, airports, and transit systems, with a substantial portion going to military-defense related matters.[30] The majority of that spending, about $404 billion, involved competitively bid contracts.[31] Because the federal government's role in procuring goods and services involves such enormous federal spending, there is a significant risk that bad actors will attempt to game the system and abuse the government's procurement process. It is difficult to say with precision how much money is lost to anti-competitive or collusive criminal conduct, but by some estimates, eliminating bid rigging could reduce procurement prices by 20%.[32] So what measures can the government take to prevent or limit procurement crimes? One answer is the PCSF.

The PCSF is the Department's coordinated, nationwide response to collusion, corruption, fraud, and other schemes that target government spending on goods and services at all levels—federal, state, and local. Moreover, the PCSF's mission reflects longstanding Department and Antitrust Division priorities including, among others, to promote competition by fairly and vigorously enforcing antitrust laws by ensuring that procurement and bidding are

30. *A Snapshot of Government-Wide Contracting for FY 2020 (infographic)*, U.S. Gov't Accountability Off. (June 22, 2021), https://www.gao.gov/blog/snapshot-government-wide-contracting-fy-2020-infographic.
31. *Id.* (comparing competed vs. non-competed).
32. *Fighting Bid Rigging in Public Procurement*, Org. for Econ. Coop. & Dev., https://www.oecd.org/competition/cartels/fightingbidriggininpublicprocurement.htm (last visited Sept. 6, 2022).

fair, open, and competitive.[33]

A. The PCSF's objectives

The PCSF has two distinct but related objectives. First: detect, investigate, and prosecute bad actors involved in antitrust and related crimes. When potential illegal conduct is identified, prosecutors and agents from the PCSF's partner agencies jointly investigate and prosecute these crimes. As the security services investigation demonstrates, the PCSF's network of skilled agents can facilitate quick and thorough prosecution of complex, international conspiracies.

Second: deter antitrust and related crimes by educating and training government officials. Procurement officials are the front lines of defense against procurement crimes, and the PCSF aims to arm them with the ability to identify red flags of collusion and bid rigging and the knowledge of what to do when they suspect misconduct. To date, the members of the PCSF have conducted hundreds of outreach meetings and trainings at a range of federal and state agencies. Outside of the United States, the PCSF Global team has delivered presentations to enforcement officials from Africa, Asia, and Europe. PCSF outreach helps enforcers preempt the collusion and fraud and also cements the PCSF in procurement officials' minds as the contact for procurement collusion questions, cases, or ideas.

B. The PCSF's enforcement tools

With both goals in mind, the PCSF uses a range of statutory tools to protect and safeguard taxpayer money from bad actors determined to rig the bidding process and defraud the government. PCSF prosecutors can charge all relevant federal crimes. They often turn to the Antitrust Division's most familiar statute, the Sherman Act, to prosecute procurement crimes involving agreements among two or more competitors to rig bids, fix prices, or allocate markets.[34]

1. Antitrust crimes

Bid-rigging schemes

Bid rigging is the most prominent antitrust crime in the procurement con-

33. *See* Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 9, 2021); *see also* U.S. Dep't of Just., Department of Justice Strategic Plan FYs 2022–2026 (last updated July 1, 2022) (Strategic Goal 4: Ensure Economic Opportunity and Fairness for All).

34. The Antitrust Division has a unique tool for encouraging corporate and individual cooperation when investigating violations of section 1: the Leniency Policy. A company or an individual can obtain immunity from prosecution, also known as "leniency," if the company or individual self reports participation in a criminal conspiracy in violation of section 1 of the Sherman Act, 15 U.S.C. § 1, *and* meets other certain conditions. The Leniency Policy is set forth in Justice Manual 7-3.300–3.430. More information about the Leniency Policy is available at https://www.justice.gov/atr/leniency-program.

text. It occurs when two or more competing companies or individuals agree to corrupt the bidding process—before the bids are submitted—by deciding which company will submit the most attractive bid (normally the lowest price) to win the contract. The other conspiring companies agree to submit less attractive bids, typically bids with higher prices. Bid rigging allows the conspirators, who are supposed to be competing, to decide effectively how much the government will pay for a contract instead of free-market competition deciding the outcome. Bid-rigging schemes typically take one of three forms: (1) bid rotation: a series of rigged contracts in which competitors take turns being the winning bidder; (2) complementary bidding (or comp bidding): competitors submitting inflated bids or otherwise unattractive bids with the intention of losing; or (3) bid suppression: competitors agreeing not to submit a bid to help a conspirator win. All three schemes generally involve competitors agreeing in advance as to who will win the contract, what the winning price will be (that is, the artificial low bidder), and which companies will submit bids at higher prices, if at all. Long-running schemes often employ a combination of these three forms.

The Security Services investigation, for instance, alleges a bid-rotation scheme in which the defendants conspired to rig the bidding by agreeing in advance which company would win certain security services contracts and the price that each competitor would bid for the contracts.[35.] The alleged scheme resulted in the DOD receiving inflated bids at non-competitive prices from the conspirators and depriving the DOD of a competitive bidding process.[36.]

Price-fixing schemes

Price-fixing schemes involve competitors agreeing to raise, fix, or otherwise maintain the price at which their products or services are sold. Price fixing can take various forms, such as an agreement among manufacturers of a particular product to charge similar prices or to raise prices, or agreements to establish minimum floor prices or establish standard pricing formulas. To prove a price-fixing conspiracy, the government is not required to prove that the conspirators agreed to charge exactly the same price. For example, an agreement by competitors to raise individual prices by a certain amount or percentage, or to maintain a certain profit margin, could constitute a price-fixing scheme even if the resulting prices are not the same. Similarly, agreements either to establish or adhere to uniform price discounts, eliminate discounts, fix co-payment fees, or fix credit terms fall under the price-fixing umbrella. In short, a price-fixing agreement includes any agreement among competitors to affect the price of a good or service.[37.]

Market-allocation schemes

Market-allocation schemes involve competitors agreeing to divide up a par-

35. *See* Seris Indictment, *supra* note 2, at 5–6.
36. *See id. at 6.*
37. *See* ATR Primer, *supra* note 26, at 3.

ticular market by geographic area, customer, or product. For instance, in customer allocation schemes, competing companies may divide specific customers so only one competitor will be allowed under the conspiratorial agreement either to sell, buy, or bid on contracts for those customers. In return, the other competitors will agree not to sell, buy, or bid on contracts for those customers.[38]

Antitrust crimes and fraud

Common sense tells us that the purpose of bid-rigging, price-fixing, and market-allocation schemes, like mail or wire fraud, is to "reap the benefit of the conspiracy: to be awarded public . . . contracts at anti competitively high prices and to be paid for those contracts."[39] Garnering illicit profits and controlling prices are the central objectives of any conspiracy to restrain trade—whether the conduct involves bid-rigging, price-fixing, or market-allocation schemes.[40]

Section 1 antitrust crimes share another hallmark with other white collar crimes: The conduct typically involves indicia of fraud such as concealment, trickery, and deceit. Indeed, when competitors agree to rig the bidding process, the bad actors trick and deceive the procurement official into believing that the corrupted bidding process is legitimate, fair, and competitive by concealing the fact of their collusion. In this sense, though frequently couched in terms of anti competitive behavior, section 1 antitrust crimes such as bid rigging are essentially crimes of fraud.[41] Furthermore, many government agencies require bidders to explicitly certify the non collusive nature of their bidding. Such certifications can often serve as a material misrepresentation to support a wire fraud charge.[42]

---

38. *Id.* at 6.
39. United States v. Northern Improvement Co., 814 F.2d 540, 542 (8th Cir. 1987).
40. United States v. Dynalectric Co., 859 F.2d 1559, 1568 (11th Cir. 1988) (highlighting "financial self-enrichment" and "garner[ing] illicit profits" as objectives of bid-rigging schemes).
41. *See Fraud*, Black's Law Dictionary (11th ed. 2019).
42. A line of cases also sets out a "pretense" theory of fraud, applicable to almost all bid-rigging, that does not require an affirmative misrepresentation, but rather is based on omitting or concealing material facts designed to induce false belief and action. *See* United States v. Weimert, 819 F.3d 351, 355 (7th Cir. 2016). Several courts have accepted this theory, particularly where the charged scheme involves "breaking the rules . . . violat[ing] fundamental notions of honesty, fair play and right dealing." United States v. Martin, 411 F. Supp. 2d 370, 373 (S.D.N.Y. 2006); *see also* United States v. Trapilo, 130 F.3d 547 (2d Cir. 1997). Bid-rigging, in the context of a competitive market, fits neatly into this theory. *See, e.g.*, United States v. Worthen, No. 17-cr-175, 2018 WL 1784071, at *1–2 (N.D. Cal. Apr. 13, 2018) (rejecting defense argument that "[s]ubmitting a high bid for a construction contract is not an act of deception" supporting a conspiracy to defraud under section 371 (alteration in original)); United States v. Anderson, 326 F.3d 1319, 1327 (11th Cir. 2003) (finding sufficient evidence of a single conspiracy to sustain convictions under 15 U.S.C. § 1 and 18 U.S.C. § 371 as "the common goal of the overarching bid rigging scheme was to steal from the United States by inflating the winning bids"); United States v. Washita

The government, however, is not required to prove that a defendant used fraud such as trickery or deceit in a section 1 antitrust prosecution. Rather, in prosecuting an antitrust bid-rigging conspiracy, the government is only required to prove three elements: (1) an agreement between two or more competitors to rig bids,[43] (2) the defendant knowingly—that is, voluntarily and intentionally—became a member of the conspiracy knowing its goals and intending to help accomplish those goals, and (3) the conspiracy involved activities within the flow of and substantially affected interstate commerce.[44] Of course, antitrust schemes are not accidents, mistakes, or misunderstandings. Rather, they are calculated decisions by conspirators to conceal, trick, and deceive the procurement official. Highlighting the fraudulent and deceitful nature of a bid-rigging scheme at trial, even if a fraud charge is not brought, emphasizes the criminality, such that an average juror can better appreciate the motivations and illegality of the charged conduct.

2. Other crimes relating to procurement collusion

Procurement collusion can take many forms. The Antitrust Division's mission is to promote and protect competition. Its criminal attorneys prosecute violations of antitrust and other federal statutes that affect the competitive process—bid rigging, price fixing, market allocation, and attempts and conspiracies to monopolize. The PCSF's mission zeroes in on conduct that undermines the procurement process. For instance, a contractor providing a government procurement official with money or other things of value in exchange for confidential inside information about the estimated costs of a contract, competitors' bid prices, or how much a contractor must bid to win the contract may constitute evidence of, among other crimes, bribery[45] or honest services fraud,[46] on top of a bid-rigging charge. Similarly, a procurement official's receipt of bribe money or other things of value could constitute income, which must be reported on federal and state income tax returns. If the procurement official filed a federal income tax return (or failed to file an income tax return) that did

---

Constr. Co., 789 F.2d 809, 818 (10th Cir. 1986) (finding that a collusive bidding scheme was the valid basis for a mail fraud conviction because it "deprived taxpayers of the monetary advantage of competitive bidding").

43. An indictment could *allege* a conspiracy to achieve two objectives—price fixing and bid rigging; however, the government need not *prove* that the conspiracy sought to achieve both objectives. Rather, the government need only prove that the conspiracy sought to achieve at least one of these objectives.

44. 15 U.S.C. § 1; *see also* United States v. Alston, D.M.D., P.C., 974 F.2d 1206, 1210 (9th Cir. 1992) (elements of criminal antitrust conspiracy); United States v. Coop. Theatres of Ohio, Inc., 845 F.2d 1367, 1373 (6th Cir. 1988) (same); United States v. Andreas, 216 F.3d 645, 669 (7th Cir. 2000) (discussing intent and jury instruction).

45. 18 U.S.C. § 201(b) (offering or accepting bribes involving a federal official); 18 U.S.C. § 201(c) (offering or accepting gratuity involving a federal official); 18 U.S.C. § 666 (bribery of a state or local official).

46. 18 U.S.C. §§ 1343, 1346 (honest services fraud).

not report the money (or other things of value), then a prosecutor might consider pursuing a criminal tax charge against the official, such as tax evasion[47] or filing a false tax return.[48] Charging a company executive with accepting bribes or requesting side payments in exchange for favors and not reporting the income is not unusual.[49] If a contractor submits invoices via email or other electronic means and receives payments for goods that were never delivered or services that were never performed, then a prosecutor may want to consider a wire fraud charge.[50] Similarly, submitting false certifications that claim, among other things, that the contractor purportedly met certain guidelines such as veteran or minority or women-owned business status may constitute a wire fraud scheme or set-aside fraud scheme.[51]

PCSF prosecutors have several statutes to pursue crimes ranging from bid-swap arrangements to bribery, money laundering, and honest services fraud involving procurement officials.[52] In its short history, the PCSF has deployed many of these tools in successful prosecutions.

C. The PCSF's track record

The PCSF staff teams of prosecutors and agents around the United States to investigate and prosecute matters affecting specific areas. To that end, the PCSF has formed national partnerships with 22 USAOs, opened more than 60 grand jury investigations since its inception in 2019, and brought a range of procurement criminals to justice.

- **Infrastructure bid rigging and fraud:** In *United States v. Brewbaker* (E.D.N.C. 2022), a jury convicted a former executive of Contech Engineered Solutions, LLC for participating in a conspiracy to rig bids and commit fraud, three counts of mail fraud, and one count of wire fraud. The defendant had rigged bids and submitted false certifications of non-collusion for more than 300 aluminum structures that the state of North Carolina funded between 2009 and 2018. Contech pleaded guilty to mail fraud and bid rigging and agreed to pay a criminal fine of $7 million and restitution of more than $1.5 million to the NC Department of Transportation.[53]

---

47. 26 U.S.C. § 7201.
48. 26 U.S.C. § 7206(1).
49. *See, e.g.*, Press Release, U.S. Dep't of Just., Former Las Vegas Casino Company Employee Sentenced to Prison (Mar. 27, 2015).
50. 18 U.S.C. § 1343.
51. *See, e.g.*, Press Release, U.S. Dep't of Just., Construction Company Owner Convicted of Fraud in Securing More Than $240 Million in Contracts Intended for Service-Disabled Veteran-Owned Small Businesses (June 30, 2022).
52. *See, e.g.*, Press Release, U.S. Dep't of Just., Commercial Flooring Company Pleads Guilty to Antitrust and Money Laundering Charges (Aug. 30, 2021).
53. Press Release, U.S. Dep't of Just., Former Engineering Executive Convicted of Rigging Bids and Defrauding North Carolina Department of Transportation (Feb. 1, 2022).

- **Army "swag" sham bids and conspiracy to defraud:** In *United States v. O'Brien* (M.D. Fla. 2022), three Florida men were indicted for allegedly conspiring to rig the bidding on customized promotional products (swag) for the U.S. Army. To carry out the scheme and secure sales for a pre-arranged winner, the defendants are alleged to have exchanged their company's bid templates and submitted bids on each other's behalf. Two of the defendants were charged with conspiring to defraud the federal government by creating shell companies that gave the false impression of competition.[54.]

- **Caltrans bid rigging and bribery:** In *United States v. Yong* (E.D. Cal. 2022), a contract manager for the California Department of Transportation (Caltrans) pleaded guilty to conspiracy and bribery regarding rigging bids on Caltrans improvement and repair contracts by ensuring that contracts went to companies controlled by the defendant's co-conspirators at inflated prices. The scheme, which impacted contracts worth more than $8 million, also involved bribery and "no-bid" contracts awarded on an emergency basis without competitive bidding.[55.]

- **Fraud at DOD installations in South Korea:** In *United States v. Kwon* (S.D. Tex. 2022), two South Korean nationals were indicted for conspiring to rig bids on subcontract work at U.S. military bases in South Korea. The indictment alleges that the defendants were officers at a construction company in South Korea that did subcontract work on U.S. military bases in the country. The alleged comp-bid conspiracy ran from November 2018 to March 2020.[56.]

- **Fraud at the U.S. Bureau of Prisons (BOP), "food for felons":** In *United States v. Porras* (C.D. Cal. 2022), a former contractor at a food supply company pleaded guilty to conspiring to rig more than 100 bids with a person at a competing food company to determine which supplier would obtain low-bid contracts from the BOP.[57.]

D. The PCSF's future

The PCSF is well-positioned to continue bringing successful cases and advancing the administration's priority of safeguarding competition.[58.]

---

54. Press Release, U.S. Dep't of Just., Three Florida Men Indicted for Rigging Bids and Defrauding the U.S. Military (Apr. 12, 2022).
55. Press Release, U.S. Dep't of Just., Former Caltrans Contract Manager Pleads Guilty to Bid Rigging and Bribery (Apr. 11, 2022).
56. Press Release, U.S. Dep't of Just., Contractors Indicted for Rigging Bids on Subcontract Work and Defrauding U.S. Military Bases in South Korea (Mar. 17, 2022).
57. Press Release, U.S. Dep't of Just., Inland Empire Man Agrees to Plead Guilty in Bid-Rigging Scheme to Obtain Contracts to Provide Food to Federal Prison Facilities (Apr. 5, 2022).
58. On July 9, 2021, President Biden issued an Executive Order on Promoting Competition in the American Economy, outlining 72 initiatives across a range of federal

The passage of the $1.2 trillion Infrastructure Investment and Jobs Act (Infrastructure Act) in November 2021 provides fresh urgency to the PCSF and procurement enforcement.[59] This injection of government spending is certain to attract bad actors, as one circuit court recently reflected: "Like bears to honey, white collar criminals are drawn to billion-dollar government programs."[60]

The Infrastructure Act spending is concentrated in industries like construction and transportation, allocating $110 billion to repair and rebuild roads and bridges; $89.9 billion to expand and improve public transit; $42 billion to upgrade and repair U.S. airports, ports, and waterways; and $65 billion to upgrade power infrastructure.[61] It is no secret that bad actors target these industries, as the PCSF's recent cases show.

Fraudsters often abuse substantial public spending programs, as seen with the COVID-19 relief programs like the Paycheck Protection Program (PPP) (2020–2022),[62] the Troubled Asset Relief Program (TARP) (2008),[63] and the Hurricane Katrina relief funds (2004–2006).[64] Sadly, with the passage of the Infrastructure Act, the risk of such fraud is not just speculative, but certain.

In response, the PCSF has expanded its roster of law enforcement partner

---

agencies aimed at tackling competition problems in specific sectors of the economy. *See* Exec. Order No. 14,036, 86 Fed. Reg. 36,987 (July 9, 2021). Reinvigorating antitrust enforcement and combatting public corruption are also emphasized in the Department's strategic plan for 2022–2026. *See* U.S. Dep't of Just., *supra* note 33 (Objective 4.1: Reinvigorate Antitrust Enforcement and Protect Consumers as well as Objective 4.2: Combat Corruption, Financial Crime, and Fraud—Strategy 2: Combat Public Corruption).

59. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021); *see also* White House, A Guidebook to the Bipartisan Infrastructure Law for State, Local, Tribal, and Territorial Governments, and Other Partners (2022).

60. United States v. Howard, 28 F.4th 180, 186 (11th Cir. 2022).

61. White House, Fact Sheet: The Bipartisan Infrastructure Deal (2021).

62. *See, e.g.*, Press Release, U.S. Dep't of Just., Justice Department Takes Action Against COVID-19 Fraud (Mar. 26, 2021); *Examining Federal Efforts to Prevent, Detect, and Prosecute Pandemic Relief Fraud to Safeguard Funds for All Eligible Americans: Hearing Before the H. Select Subcomm. on the Coronavirus Crisis*, 117th Cong. (2022).

63. *See, e.g.*, Off. of the Special Inspector Gen. for the Troubled Asset Relief Program, Semiannual Report to Congress October 1, 2021 – March 31, 2022, at2 (2022) ("SIGTARP investigations have resulted in the recovery of more than $11.3 billion while coordinating with the Department of Justice (DOJ) and other law enforcement agencies to criminally prosecute 467 defendants."); Press Release, U.S. Dep't of Just., United States Settles False Claims Act Action Against Estate and Trusts of Layton P. Stuart for $4 Million (Oct. 16, 2015).

64. *See, e.g.*, Press Release, U.S. Dep't of Just., Two Individuals Indicted on Charges of Conspiracy and Bribery in Connection with a U.S. Army Corps of Engineers New Orleans Levee Reconstruction Project (May 15 2008); *see generally Hurricane Katrina: Waste, Fraud, and Abuse Worsen the Disaster: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affs.*, 109th Cong. (2006).

agencies around the country and abroad. Additionally, the PCSF is focusing on outreach and training to a more diverse range of procurement officers, auditors, and accountants to broadly educate and inform the civil service on the problem of procurement crimes. Such outreach typically provides a basic overview of federal antitrust law, introduces classic procurement collusion schemes, discusses recent cases, and highlights red flags of collusion. PCSF attorneys and agents frequently partner to provide the perspectives of the prosecutor and investigator. The PCSF has made hundreds of presentations to more than 20,000 agents and procurement officials over the last two years.

III. Conclusion

Bad actors will always seek ways to defraud the government and steal taxpayer dollars. Deterring and prosecuting procurement crime is a national priority given the billions of dollars that the federal government spends on contracts every year. The PCSF plays a critical role in helping to investigate and prosecute bad actors and educating and training government procurement officials. The PCSF has shown that prosecutors and law enforcement agents can work together on complex criminal investigations involving public procurement fraud, even when the crimes occur halfway around the world amid a global pandemic. As the Security Services investigation highlights, there is no market too foreign or too exotic for procurement crime, and so there is no market the PCSF will ignore.[65.]

About the Authors

Philip Andriole is a Trial Attorney in the New York Office of the Antitrust Division, where he has served since 2019. Mr. Andriole also served as a Special Assistant U.S. Attorney at the Eastern District of Virginia USAO from March 2020 to November 2020.

Chris Maietta is a Trial Attorney in the New York Office of the Antitrust Division, where he has served since 2016. From 2002 to 2016, Mr. Maietta served as a Trial Attorney in the Department's Tax Division, Criminal Enforcement Section, in Washington, D.C., where he investigated and prosecuted criminal tax fraud cases in various districts across the United States from San Diego to Boston and many locales in between.

The authors thank Antitrust Division Trial Attorney Bryan Serino for sharing his experience on security services.

65. See *Procurement Collusion Strike Force*, *supra* note 3, to learn more about the PCSF, report suspicions, or request training.

Page Intentionally Left Blank

Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology

Sanjeev Bhasker
United States Digital Currency Counsel, Digital Currency Initiative
Money Laundering and Asset Recovery Section
National Cryptocurrency Enforcement Team

Alexandra D. Comolli
Assistant United States Attorney
Digital Asset Coordinator
Southern District of Florida

Olivia Zhu
Trial Attorney
Money Laundering and Asset Recovery Section

Digital assets and blockchain technology are some of the great innovations of our time. Criminals, as they have with many great innovations, unsurprisingly co-opt these inventions as tools to achieve their own malicious ends. Like the gangsters of the early 20th century, today's criminals exploit these world-changing technologies to expand or establish their criminal enterprises. But unlike their 20th century predecessors who employed widely available fast-moving cars and Thompson submachine guns, criminals today exploit digital assets and blockchain technology on a mind-boggling level.[1] They do so as the supporting technologies evolve at an incredible rate, leading to even more creative opportunities for illicit use.[2]

As prosecutors face down a tidal wave of criminal activity in this area, our

1. *The FBI and Crypto: Cyberattacks, Ransomware and Fighting Crime in the Digital Age*, TRM Labs, Inc. (June 30, 2021), https://www.trmlabs.com/post/register-now-the-fbi-and-crypto.; *see* Jonathan Reed, *Is Anyone Doing Anything About the Explosion in Crypto Crime?,* Sec. Intelligence (Mar. 9, 2022), https://securityintelligence.com/articles/crypto-crime-solutions/; *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity,* Chainalysis: Chainalysis Rsch. (Jan. 6, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.
2. Janet L. Yellen, U.S. Sec'y of Treasury, Remarks at Am. Univ.'s Kogod Sch. of Bus. Ctr. for Innovation on Digital Assets (Apr. 7, 2022).

hope is to demystify digital asset investigations. Emerging technologies may also lead to opportunities for prosecutors to employ tried and true investigative methods. We provide here a general roadmap that addresses the most common initial questions asked when considering a prosecution involving digital assets and encourages prosecutors and investigators to rely on their common sense and "traditional" litigation experiences. Each investigation consists of collecting and analyzing evidence, sharing evidence with defense counsel through discovery, and ultimately admitting evidence at trial and other related hearings. To be sure, our efforts here are not and cannot be exhaustive (fear not, editors, we will heed our page limit). Our colleagues in this space have provided significant contributions, and we do not parrot here the issues they so adeptly addressed. Rather, we provide a starting point for those brave and inquisitive souls diving into the whirlwind world of digital assets. Buckle up, friends. This is gonna be a wild ride.

I. The initial S.O.S.—who to call

Let's start with some very good news—you are not alone. You have many colleagues willing to share their vast expertise with you. In fact, you might peek your head out of your office and find the counsel you seek just down the hall.

Your first lifeline is your office's Digital Asset Coordinator (DAC), who serves as the regional subject-matter expert on digital assets and a first line of information and guidance about legal and technical matters related to these technologies.[3] As questions arise throughout your prosecution, particularly around applying existing authorities and laws to digital assets (for example, search and seizure warrants, restraining orders, criminal and civil forfeiture actions, indictments, and other pleadings), your office's DAC is there to guide you through the legal and technical hurdles. As a member of the DAC Network, the DAC engages with other experts in United States Attorney's Offices (USAOs) across the country, addressing new developments in the digital asset space and exchanging training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes.

Because the technology is rapidly evolving, you may need to seek even more specialized assistance from other Department of Justice (Department) components. Here again, you are in expert hands. The Money Laundering and Asset Recovery Section's (MLARS) Digital Currency Initiative (DCI) has long been a go-to resource for those seeking expert advice regarding all things blockchain and digital assets—including money laundering, seizure, and forfeiture matters. In 2018, MLARS developed the DCI, which specializes in cryptocurrency-related prosecutions, including the recovery of cryptocurrency assets.[4] The DCI provides both international and domestic legal guidance and

3. Press Release, U.S. Dep't of Just., Justice Department Announces Report on Digital Assets and Launches Nationwide Network (Sept. 16, 2022).
4. U.S. Dep't of Just., Report of the Attorney General's Cyber Digital Task Force 100–01 (July 2018).

support to investigators, prosecutors, and government agencies on cryptocurrency prosecutions, seizures, and forfeitures. Additionally, the DCI provides cryptocurrency-related training and engages in policy dialogue concerning legislation, forfeiture, and prosecution. Building on this Initiative, in October 2020, the Department issued the Attorney General's Cryptocurrency Enforcement Framework articulating the concerns and challenges associated with this emerging technology.[5]

To assist with the more complex and large-scale prosecutions, the Department announced the creation of the National Cryptocurrency Enforcement Team (NCET) in October 2021, "to tackle complex investigations and prosecutions of criminal misuses of [digital assets], particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors."[6] This team of experienced federal prosecutors assists with, among other things, developing investigative and prosecutorial strategies, and providing legal guidance to the field.

Understanding the importance of trial-tested resources, we direct your attention to the Department's MLARS DCI, Computer Crime and Intellectual Property Section (CCIPS), and NCET's websites. Each provides go-bys to assist with digital asset investigations and trial litigation.

II. Exploring (un)known lands: Has anyone done this before? And do they have a map?

Like Chuck Noland in *Cast Away*, attorneys cling to our "Wilson"—legal precedent.[7] When developing the legal theory of a case or an argument, attorneys immediately (and rightfully) ask, "Has anyone done this before?" and begin their legal research through this narrow lens. While the breadth of digital asset and blockchain-related precedent is growing, there are undoubtedly many legal questions evolving. These questions often warrant familiar answers. Rest assured, we still have our trusty "Wilson" at the ready. We simply need a wider lens. The question is not, "Has anyone done this before," but instead, "How do I argue the technology and facts when applied to 'X,' 'Y,' or 'Z' precedent?" To bridge the gap, prosecutors must take special care to understand this new technology and existing precedent. Only then can we make an informed argument and employ the proper precedent. Remember, digital asset or blockchain technology-related precedent is still nascent when compared with that involving the U.S. dollar or other traditional financial instruments. What you do here matters. As in any area where a prosecutor or other lawyer is unfamiliar: Don't just sit there; ask questions, the hard questions. Mind the

5. *See generally* U.S. Dep't of Just., Cryptocurrency: Enforcement Framework (Oct. 2020).
6. Press Release, U.S. Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team (Oct. 6, 2021).
7. Cast Away (DreamWorks Pictures 2000) (In the movie, Wilson—a volleyball—serves as Chuck Noland's anthropomorphized buddy during the four years that Noland is stranded on a deserted island.).

details. As the New England Patriots say, "Do your job."[8]

As has plagued other innovations, digital assets and blockchain technology are exploited for all manners of criminal conduct, including nation-state[9] and terrorist activity,[10] fraud,[11]
human trafficking,[12] child exploitation,[13] and drug trafficking.[14] Whatever the underlying criminal scheme, digital assets are commonly used to move and store value—and where there is movement of value, there is the potential for money laundering. Thus, we look to anti-money laundering regulations. Two notable pillars of U.S. law address this conduct: the Bank Secrecy Act[15] and the Money Laundering Control Act.[16] The former focuses on regulating financial gatekeepers, such as banks and money service businesses, while the latter criminalizes money laundering itself. For a more extensive overview of digital asset-enabled money laundering, we recommend turning to "*Surfing the First Wave of Cryptocurrency Money Laundering*," which appeared in the May 2021 edition of this Journal.[17]

While inquiring "if anyone has done—or is anyone doing—this," it is important to consider our sister litigating components and possible parallel investigations. The United States Department of Treasury's Financial Crimes Enforcement Network (FinCEN), for instance, plays a prominent role in regulating this space, ensuring gatekeepers register and comply with their anti-money laundering recordkeeping obligations—and taking action when they do

---

8. *See* NFL Network, *Do Your Job: Bill Belichick and the 2014 Patriots*, YouTube (Aug. 13, 2015), https://www.youtube.com/watch?v=bwSlEvG0ngo.
9. Verified Complaint for Forfeiture *In Rem*, United States v. 113 Virtual Currency Accts., No. 20-cv-606 (D.D.C. Mar. 3, 2020), ECF No. 1; *e.g.*, Press Release, U.S. Dep't of Just., Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 19, 2020).
10. *E.g.*, Press Release, U.S. Dep't of Just., Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020).
11. *E.g.*, Press Release, U.S. Dep't of Just., Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving over $100 Million in Intended Losses (June 30, 2022).
12. *E.g.*, Press Release, U.S. Dep't of Just., Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment (Apr. 9, 2018).
13. *E.g.*, Press Release, U.S. Dep't of Just., South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which Was Funded by Bitcoin (Oct. 16, 2019).
14. *E.g.*, Press Release, U.S. Dep't of Just., AlphaBay, the Largest Online "Dark Market," Shut Down (July 20, 2017).
15. Currency and Foreign Transactions Reporting Act of 1970 (*Bank Secrecy Act*), Pub. L. No. 91-508, 84 Stat. 1114.
16. Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207, 3207–18.
17. *See generally* Alexandra D. Comolli & Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DOJ J. Fed. L. & Prac., no. 3, 2021.

not.[18] Other components and statutes may also be involved depending on, inter alia, the functionality, governance, and purpose of the underlying technology, particularly as digital assets continue to develop and evolve into uses beyond the movement and storage of value into broader applications such as decentralized finance or non-fungible tokens (NFTs).[19] For example, the Securities and Exchange Commission has viewed certain digital assets as securities under the Securities Act of 1933 and Securities and Exchange Act of 1934 for some time, employing the *Howey* test[20] to make its threshold determination as to whether the asset qualifies as a security.[21] So, too, has the Commodities and Futures Trading Commission long found that Bitcoin is a commodity under the Commodity Exchange Act.[22] Prosecutors should note that a particular criminal scheme may trigger multiple statutes and components discussed here, as one could imagine, because a digital asset that is a security or a commodity could also be used as a vehicle for money laundering. As a result, parallel investigations between sister components may arise. Notifying your office's DAC is a great starting point to recognize and work through case deconflictions.

III. Jumping right in—blockchain analysis and digital asset investigations

As mentioned above, many of our colleagues have addressed digital asset investigative strategies and evidence admission in previous editions of this publication.[23] These articles, written by experienced federal prosecutors, describe

18. Press Release, U.S. Dep't of Treasury, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales (July 26, 2017); U.S. Dep't of Treasury, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001) (May 9, 2019); U.S. Dep't of Treasury, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (FIN-2013-G001) (Mar. 18, 2013).

19. Bitcoin is no longer the only game in town and has not represented the majority of digital asset transaction volume since 2016. In 2022, the overwhelming majority of transactions have involved stablecoins or cryptocurrencies with the smart contract functionality that powers decentralized finance and Web3. *See* Chainalysis, The Chainalysis State of Web3 Report (2022).

20. Sec. & Exch. Comm'n v. W.J. Howey Co., 328 U.S. 293 (1946).

21. Sec. & Exch. Comm'n, Framework for "Investment Contract" Analysis of Digital Assets (2019).

22. Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions, Coinflip, Inc. & Francisco Riordan, CFTC Docket No. 15-29 (Sept. 17, 2015).

23. *See, e.g.*, Matthew J. Cronin, *Hunting in the Dark, a Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 U.S. Att'y Bull. (July 2018); Michele R. Korver, C. Alden Pelker & Elisabeth Poteat, *Attribution in Digital Asset Cases*, 67 DOJ J. Fed. L. & Prac., no. 1, 2019; Neal B. Christiansen & Julia E. Jarrett, *Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset*, 67 DOJ J. Fed. L. & Prac., no. 3, 2019; C. Alden Pelker, Christopher B. Brown & Richard M. Tucker, *Using Blockchain Analysis From Investigation to Trial*, 69 DOJ J. Fed. L. & Prac., no. 3, 2021; Comolli & Korver, *supra* note 17.

in detail evidentiary rules and specific strategies for prosecuting such cases. Our focus here is not to rehash these methods, but rather to encourage their applications in investigations and trial litigation. A great place for us to start is blockchain analysis and domestic versus foreign legal process.

A. Blockchain analysis

Much is made of "blockchain analysis" in the digital asset world. Even its name can sound quite daunting. But recall the original Scooby Doo cartoons—the Scooby Gang often unmasked the culprit to reveal a familiar face. While the Scooby Gang's tactics were not always in line with the rigorous standards of American jurisprudence, perhaps there is some investigative wisdom gained from their adventures. For when we unmask the mysterious blockchain analysis, we find a familiar investigative technique: following the money.[24] Oh, thank goodness! A traditional investigative technique. Yes, many criminal cases begin and end successfully when investigators "follow the money." While effective blockchain analysis requires proficient training and expertise, it need not be quite so frightening. In fact, this technique can be used both to identify criminal actors and to build a case against them.[25]

The public blockchain enables investigators to trace funds forwards and backwards from a single address or a single transaction, akin to how investigators trace the movement of funds in fiat currencies.[26] Yet, unlike more traditional bank records, the blockchain does not identify the sender or receiver, apart from the public addresses. It is here that blockchain analysis brings the great irony of digital assets front and center: The need to cash out (that is, convert) digital assets into traditional currency remains the reality.[27] Some virtual asset service providers (VASPs), such as cryptocurrency exchanges, provide the all-important on and off ramps connecting the "real world" and the "virtual world." VASPs, which are generally recognized as money service businesses (MSBs) domestically, are regulated in the United States under the Bank Secrecy Act and respond to legal process with valuable attribution evidence—a result of their anti-money laundering recordkeeping obligations (thank you, FinCEN!).[28]

B. Domestic vs. foreign legal process

At the onset of a case involving digital assets, the investigative team should discuss basic parameters of collecting and storing evidence, serving legal process, and documenting these materials in real time. As in traditional evidence collection, prosecutors should remain mindful of organizing evidence in an in-

24. Christiansen & Jarrett, *supra* note 23, at 165.
25. Pelker et al., *supra* note 23, at 64; Christiansen & Jarrett, *supra* note 23, at 165–170.
26. Comolli & Korver, *supra* note 17, at 213.
27. *Id.* at 213–14.
28. U.S.Treausry Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies: FinCEN Guidance (2019).

telligible way that can be later shared with defense counsel and the court or jury.

When gathering evidence, prosecutors must distinguish between domestic and foreign legal service of process. While most prosecutors are familiar with domestic evidence collection, given the growing number of internationally located digital asset exchanges,[29] international record requests are increasingly more prevalent and require specific procedures. Service of foreign legal process must involve the Department's Office of International Affairs (OIA), which assists as our Central Governing Authority for, among other things, lawfully obtaining foreign records and property (for example, digital assets).[30] Their guidance at the onset of your investigation will help greatly when sharing evidence and ultimately seeking the court's permission to admit records at trial. Among OIA's benefits, including sound institutional knowledge of diplomatic and legal relations, they assist with serving U.S. subpoenas and seizure requests on foreign counterparts as well as serving Mutual Legal Assistance Treaties (MLATs), which are often necessary when admitting evidence in court. Once a prosecutor determines that a specific digital asset exchange is located internationally, and they wish to serve a subpoena or seizure warrant on this exchange to gather records or digital assets, they should then contact OIA to discuss the best country-specific procedures before acting. Once this analysis is completed, we move forward with confidence that the investigation's evidence should be admitted in court.

IV. Now presenting . . . the evidence: How would this work at trial?

While we cannot revisit every trial strategy in this article, we focus on emerging trends in digital asset litigation. Prosecutors should embrace digital asset trial preparation with the same diligence required of any criminal case.[31] Once in court, a prosecutor presents their case in an intelligible format to an impartial jury or judge. This process begins with an overview of the investigation, a presentation of facts and their application to the law, and an ultimate advocacy for disposition.[32] Generally, a foundational background of digital assets and blockchain analysis, combined with pertinent case facts, helps forecast

29. *See* CoinMarketCap, https://coinmarketcap.com/rankings/exchanges/ (last visited Nov. 7, 2022).
30. *See Off. of Int'l Affs.,* U.S. Dep't of Just., https://www.justice.gov/criminal-oia/office-international-affairs#:~:text=The%20Office%20of%20International%20Affairs,U.S.%20criminal%20investigations%20and%20prosecutions (last updated June 9, 2015).
31. Prosecutors should consider submitting a pre-trial brief to the court discussing evidentiary issues and allowing the judge to familiarize themselves with more technical matters before trial.
32. *See* Off. of U.S. Att'ys, U.S. Dep't of Just., *Justice 101: Trial*, https://www.justice.gov/usao/justice-101/trial (last visited Nov. 7, 2022).

your case-in-chief.

Additionally, one of the many unique characteristics of digital asset evidence is the decentralized and open-source features of blockchain records.[33] A fortunate fact is that most blockchains contain publicly available, immutable records of digital asset transactions.[34] This information is readily verifiable on a respective blockchain, shareable with defense counsel, and also useful in reverse proffers when discussing the strengths of a case. Furthermore, law enforcement's ability to draft a supplemental report that further explains digital asset transactions will go a long way to assist a non-digital-asset-literate defense counsel in case disposition.

Again, like traditional criminal litigation, here a prosecutor is simply intelligibly sharing evidence with opposing counsel for them to advise their client. Prosecutors are encouraged to use summary charts and other visuals, where appropriate, to assist counsel and their client.[35] A combination of substantive blockchain records, supplemental reports explaining these records, and visual summary charts help communicate the strength of one's case in the discovery stages and can assist with pre-trial disposition.

It is recommended that the trial team incorporate a digital asset designated witness, often a lay witness (for example, a case agent or someone familiar with the technology), to testify about digital assets and blockchain fundamentals at the onset of your presentation.[36] This witness assists the trier of fact with understanding technology and its application in your case-in-chief. That lay witness, in addition to other fact witnesses, can also explain the specific evidence in your investigation. Through this testimony, prosecutors admit trial evidence and establish a record of digital asset transactions (akin to a traditional financial investigation, but instead with blockchain analysis). Like a drug chemist testifying about a narcotic's chemical balance, explaining its chain of custody and testing procedures and then opining on the narcotic's identity and purity levels, a digital asset witness will walk the trier of fact through the identification, analysis, and applications of digital asset transactions. While blockchain expert witnesses can be used and qualified as such, they are often not necessary given the straightforward nature of this immutable evidence. If the prosecutor desires to discuss the value of a Rule 702 expert, we recommend consulting with their office's DAC. Once evidence is admitted, the prosecutor then advocates for the jury to follow the evidence or digital asset transactions, leading to the defendant's attribution.[37]

In separate hearings (that is, sentencing or suppression hearings), prosecutors are encouraged to use the same format when addressing the court, to wit presenting foundational background of a digital asset's technology, explaining the contested facts and admitting the evidence, and then advocating why spe-

33. See open-source sites like Blockchain.com and Etherscan.io for more.
34. *See, e.g.*, United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020).
35. *See* Pelker et al., *supra* note 23, at 96.
36. *See* Cronin, *supra* note 23, at 65; Pelker et al., *supra* note 23, at 92.
37. *See* Korver, *supra* note 23, at 251.

cific records and evidence should be relied on for disposition. Our hope is that as prosecutors, courts, and juries gain more familiarity with digital asset investigations, the mystique is lifted and an appreciation for digital asset litigation's reliability arises.

Finally, we turn to a brief—albeit important—discussion of seizure and forfeiture matters.

V. Who holds the private keys? Seizure and forfeiture-related matters

Seizure and forfeiture are critical aspects to consider when prosecuting digital asset cases. The events of the last year alone indicate why: In the past 12 months, the Department has seized billions of dollars and forfeited tens of millions more from just a few digital asset cases.[38] Effort is required to trace, seize, and forfeit digital assets; planning ahead can ultimately pay big dividends, both figuratively and literally. Beyond the large dollar value recoveries, there are two important reasons to seize and forfeit digital assets. First, doing so deprives criminals of their ill-gotten gains.[39] Even if the government is unable to sell or liquidate the seized digital asset, seizure and restraint prevents offenders from facilitating future crimes through this property or profiting from offense proceeds; forfeiture operates as punishment for criminal conduct.[40] Second, recovered assets can be used to compensate victims.[41] Again, our colleagues have provided a useful in depth discussion of the seizure and forfeiture of digital assets in the September 2019 edition of this Journal.[42] This Part, then, will briefly touch on a few key points and new developments.

Who holds the private keys is the driving question behind digital asset seizures. Because control of the private key(s) provides the ability and authority to transfer funds (akin to account signatory authority or a super-strong PIN),[43] properly identifying their location is paramount to a successful seizure and forfeiture process. There are two important factors when considering the location of the private keys: whether the digital asset in question is held by

38. Chris Strohm & Olga Kharif, *DOJ Seizes 3.6 Billion in Bitcoin Stolen in Bitfinex Hack*, Bloomberg (Feb. 8, 2022), https://www.bloomberg.com/news/articles/2022-02-08/doj-seizes-3-6-billion-in-bitcoin-stolen-in-2016-bitfinex-hack; MK Manoylov, *Federal Prosecutors Forfeit $34 Million in Crypto Tied to Illicit Dark Web Activities*, The Block (Apr. 5, 2022), https://www.theblockcrypto.com/linked/140700/federal-prosecutors-forfeit-34-million-in-crypto-tied-to-illicit-dark-web-activities; Alexander Mallin & Luke Barr, *DOJ Seizes Millions in Ransom Paid by Colonial Pipeline*, ABC News (June7, 2021), https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821.
39. U.S. Dep't of Just., Asset Forfeiture Policy Manual § I.A (2021).
40. United States v. Libretti, 516 U.S. 29, 39 (1995).
41. *See* U.S. Dep't of Just., *supra* note 39, at ch. 14.
42. Christiansen & Jarrett, *supra* note 23, at 159.
43. *Id.* at 170; U.S. Dep't of Just., *supra* note 39, at 27; Cronin, *supra* note 23, at 67; Christiansen & Jarrett, *supra* note 23, at 157–58.

a third party (hosted) or held by the individual (unhosted); and whether the asset is located within the United States or abroad.

Once probable cause for seizure is established, hosted wallets within the United States can be seized with a seizure warrant served on the third party (that is, the VASP hosting the cryptocurrency).[44] Unhosted wallets, however, may take various forms: The private keys can be written on slips of paper, or they can be stored on software or hardware wallets, among other ways. In these cases, when the unhosted wallet is located within the United States, prosecutors should keep in mind that a warrant will be served at the wallet's location. As such, if the wallet is located within the district, prosecutors may seize the digital assets either through a standard Rule 41 search warrant[45] that authorizes the search for or seizure of digital assets (in addition to the subsequent transfer of funds from the wallet to a law enforcement unhosted wallet), or through a forfeiture seizure warrant.[46] If the wallet is located outside the district, prosecutors can still use a forfeiture seizure warrant but will need to partner with the local USAO to obtain a Rule 41 search warrant. Finally, either a hosted or unhosted wallet located abroad should only be seized in consultation with OIA and via MLAT.[47] Tread carefully with international exchanges that have a U.S. office or point of contact that is willing to accept service. Any restraint must be voluntary and should occur only after consulting with your office's Asset Forfeiture Chief, and any assets should be transferred only after a seizure warrant is served via MLAT.[48] Where questions arise, in addition to discussing with your office's DAC and Asset Forfeiture Coordinator, our colleagues at MLARS DCI and the NCET are just a phone call away and glad to help.

It is essential to remember that there may be more than one copy of the private key, so post-seizure precautions must be taken to prevent either targets or co-conspirators from quickly moving or liquidating digital assets. Once digital assets are seized, they should be transferred to an agency-controlled wallet. When doing so, agents should follow their agency's written policies. Again, preparation and planning are essential. Agents should prepare wallets in advance and determine whether the seized digital assets can and should be transferred to a government-controlled wallet. Later, when ready for liquidation, the assets can be transferred to the custody of the United States Marshals Service (USMS) for liquidation. Notably, the seizure of NFTs may present novel issues and should be coordinated with the USMS and MLARS

44. Christiansen & Jarrett, *supra* note 23, at 175–76.
45. Keep in mind that private keys can be stored in multiple formats (that is, on slips of paper, cell phones, or small hardware devices). As such, prosecutors and agents should prepare accordingly and consider search warrants that authorize the search of a person, electronic device, or both.
46. Christiansen & Jarrett, *supra* note 23, at 173–75.
47. *See* Section III.B., *supra*; *see also* Christiansen & Jarrett, *supra* note 23, at 156, 176–77.
48. U.S. Dep't of Just., *supra* note 39, at 29.

DCI.[49]

Agents and prosecutors should generally avoid liquidating digital assets before forfeiture.[50] Although some exchanges can cash out account contents in the form of a cashier's check or wire transfer, digital assets should instead be held in their original form and transferred to a government-controlled wallet. Yet digital assets are also notoriously volatile.[51] As such, parties may wish to liquidate seized digital assets before a final order of forfeiture is entered to preserve its value. In those circumstances, and if all potential claimants to the property agree, the parties may move for an interlocutory sale order only after consulting with MLARS.[52]

Just like cars, homes, cash, and myriad other properties, digital assets can be forfeited. Prosecutors should be careful to develop a theory of the underlying crime and corresponding forfeiture statutes early in the investigation to ensure successful forfeiture at the conclusion of the case. If known, the amount and type of digital assets should be listed in the indictment or bill of particulars as well as the plea agreement. Similarly, the preliminary and final orders of forfeiture should list digital assets just as they might list any other monetary asset.[53] In some situations, seized digital assets may skyrocket in value during the pendency of the investigation and case. The appreciation in value of the various seized assets may still be forfeited, no matter how substantial the increase may be.[54] For examples of plea language that addresses the issue of appreciation, please contact MLARS/DCI.

VI. Conclusion

And here we come to the end of our overview. The coming digital asset tidal wave presents us with two options: resist or flow. The choice is ours, and preparation is key. If you remember nothing else from these pages, remember this: You already have the litigation experience, necessary tools, and support of your expert colleagues to successfully figure out this "new crypto thing." To paraphrase one of the great cinematic underdogs, "[You've] been ready for this

---

49. The first known NFT seizure occurred earlier this year, when the U.K. tax authority seized three NFTs regarding a tax fraud case. *See* Anita Hawser, *UK Law Agents Seize NFTs,* Glob. Fin. (Mar. 3, 2022), https://www.gfmag. com/magazine/march-2022/uk-law-enforcement-seize-nfts.

50. U.S. Dep't of Just., *supra* note 39, at 29.

51. Jack Denton, *Bitcoin Is on a Bumpy Ride. Why Cryptos May Get Even More Volatile*, Barron's (June 15, 2022), https://www.barrons.com/articles/bitcoin-cryptos-derivatives-volatile-51655301716.

52. U.S. Dep't of Just., *supra* note 39, at 29.

53. *See, e.g.*, Verified Complaint for Forfeiture *In Rem*, United States v. Cazes, No. 17-cv-967 (E.D. Cal. July 19, 2017), ECF No. 1.

54. *See, e.g.*, United States v. Hawkey, 148 F.3d 920, 928 (8th Cir. 1998) (if property is subject to forfeiture as property traceable to the offense, it is forfeitable in full, including any appreciation in value since the time the property became subject to forfeiture; the reason for the appreciation does not matter, as the defendant may be made to pay money judgment or forfeit traceable property, but not both).

[your] whole life."[55.]

Carpe crypto.

About the Authors

Sanjeev Bhasker serves as U.S. Digital Currency Counsel with the US Department of Justice's Digital Currency Initiative (DCI) and National Cryptocurrency Enforcement Team (NCET), providing legal guidance and support to investigators, prosecutors, and government agencies on cryptocurrency prosecutions, seizures, and forfeitures. He previously served as an Assistant U.S. Attorney, providing trial and appellate litigation throughout the United States in the Western District of North Carolina and the Southern District of Texas.

Alexandra D. "Ali" Comolli is an Assistant United States Attorney and Digital Asset Coordinator for the Southern District of Florida. Previously, AUSA Comolli served approximately nine years with the Federal Bureau of Investigation, where she specialized in the investigation of virtual currency money laundering and worked alongside truly excellent case agents and prosecutors to develop innovative investigative strategy, identify otherwise-anonymous targets, and seize illicit proceeds. As a founder the FBI's Virtual Currency Response Team, she assembled an elite group of experts assigned to assist the FBI's most complex virtual currency investigations. AUSA Comolli is a graduate of Duke University and the Antonin Scalia Law School at George Mason University and is admitted to the Massachusetts bar.

Olivia Zhu is a Trial Attorney in the Money Laundering and Asset Recovery Section of the Criminal Division. She joined the Department in 2020 through the Attorney General's Honors Program as an Asset Forfeiture Fellow, and she received her J.D., cum laude, from the New York University School of Law.

55. Rudy (TriStar Pictures 1993).

Note from the Editor-in-Chief

We here at the Office of Legal Education, Publications Unit, hope that you enjoy this issue of the *Department of Justice Journal of Federal Law and Practice*. As Mandy Riedel wrote in the Introduction, prosecuting those who profit from white-collar crime, particularly corporate crime, is a top priority for the Department. To that end, this issue spotlights some of the complex issues in white-collar crime and fraud, including the attorney–client privilege and the crime–fraud exception, the Foreign Corrupt Practices Act, and the cutting-edge topic of cryptocurrency.

I'd like to introduce the new team that puts the *DOJ Journal* together and makes my job as editor-in-chief easy. Jan van der Kuijp, a member of the Attorney General's Honors Program, is our managing editor who oversees daily operations. He's assisted by Kari Risher, our University of South Carolina contractor, who acts as associate editor. They're joined by University of South Carolina law clerks Rebekah Griggs, Lillian Lawrence, Kyanna Dawson, and William Pacwa. And I would be remiss in not mentioning Jim Scheide, the USC IT wizard behind the scenes, who helps make our publication look great.

Speaking of this law journal's look, regular readers might notice that this issue is different. That's because it's our first issue published using LaTeX, a computer typesetting system based on a program originally created by Donald Knuth, a prize-winning mathematics professor at Stanford University. In the 1970s, Knuth, unhappy with the way his publisher typeset his books, spent years teaching himself the art of typography and designing a state-of-the-art computer program.[1] I'm confident that you'll agree his efforts were worth it. This issue, using an expanded version of Knuth's original program and the Palatino typeface, has a fresh, modern appearance.[2]

We couldn't have produced this issue without the hard work of our authors, all subject matter experts on white-collar crime and fraud topics. And we'd especially like to thank Mandy Riedel and Seth Wood for acting as points of contact. They recruited our authors and reviewed their articles to ensure consistency with DOJ policy and guidance. But most of all, thanks to our readers, both inside and outside of the Department, who inspire us.

As the year draws to a close, our staff hopes that you and yours have a happy holiday season. We'll see you in 2023!

Chris Fisanick
Columbia, South Carolina
December 2022

---

1. *Donald Knuth,* Wikipedia, https://en.wikipedia.org/wiki/Donald_Knuth (last visited Dec. 5, 2022).
2. My informal survey revealed that the law review published by Case Western Reserve University Law School is the only other U.S. law review that uses LaTeX. Dr. Knuth received his bachelor's and master's degrees from Case Western.