DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 66 October 2018 Number 5

United States
Department of Justice
Executive Office for United States Attorneys
Washington, DC 20530

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

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:
66 DOJ J. FED. L. & PRAC., no. 5, 2018.

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

Page Intentionally Left Blank

Corporate Crime

In This Issue

Corporate Crime

In This Issue

Introduction

Rod J. Rosenstein
Deputy Attorney General of the United States

In a 1940 speech, Attorney General Robert Jackson said, "Every person who believes, as I do believe, in a system of free private enterprise knows that government must take steps to keep it free and to keep it within the rules of the game."[1]

This issue of the Department of Justice's newly-formatted *Journal of Federal Law and Practice* shows that the Department is doing just that.

We are fighting corporate fraud and white collar crime with energy and resolve. In 2018, the Department increased white collar prosecutions over the prior year, charging more than 6,500 defendants.[2]

This volume of our new *Journal* contains articles about corporate crime written by Department professionals from Main Justice and nine of our United States Attorneys' Offices, located in every region of the nation.

The articles describe the dedicated efforts of our lawyers and agents to attack some of our most pressing law enforcement problems: health care fraud, criminal use of cryptocurrency, securities and commodities fraud, foreign bribery, and corporate accountability for the opioid epidemic. The articles discuss prosecutions of culpable individuals, appellate issues, asset forfeiture, developments in case law, and discovery in the digital age.

Most companies want to do the right thing, and our policies create incentives for corporate cooperation, remediation, and compliance. Nonetheless, white collar cases are often challenging to investigate and prosecute. They require skill, commitment, and collegiality by our agents, prosecutors, and support staff.

On behalf of the Department of Justice, I want to thank everyone who works tirelessly to deter crime and protect American consumers, investors, and taxpayers. Your efforts make a difference.

---

[1] Robert H. Jackson, Att'y Gen., Address at the Forum Meeting of the National Institute of Government (May 3, 1940).

[2] Press Release, U.S. Dep't of Justice, Justice Department Smashes Records for Violent Crime, Gun Crime, Illegal Immigration Prosecutions; Increases Drug and White Collar Crime Prosecutions (Oct. 17, 2018).

Page Intentionally Left Blank

Prosecution of Individuals in Corporate Criminal Investigations

Thomas L. Kirsch II
United States Attorney
Northern District of Indiana

David E. Hollar
Chief, Appellate Division
Northern District of Indiana

I. Introduction

Prosecutors investigating business entities for criminal wrongdoing are almost always confronted with difficult charging decisions in the course of their investigations. Among the key decisions are whether to charge individuals with crimes for their roles in an entity's wrongdoing and, if so, who to charge.

This article reviews the Department's policies regarding the charging of individuals for corporate crimes. After discussing the potential pitfalls and roadblocks to successfully charging individuals for an entity's misdeeds, it points to techniques and strategies the federal law enforcement community and its partners can use to ensure culpable individuals who victimize others by acting on behalf of their corporations are properly held accountable.

II. The goals of individual prosecutions for corporate crimes

As the Attorney General recently observed, "It is not merely companies, but specific individuals who break the law."[1] Corporations act through their owners, board members, directors, supervisors, or other management officials. Often, those individuals act with sufficient mens rea to justify individualized punishment. At the same time, the nature of the business world and the corporate decision making process can make it difficult to assign culpability for a company's crimes to any single individual, or even a collective group of individuals. In 2016, the Department convicted 132 business

[1] Jeff Sessions, Att'y Gen., U.S. Dep't of Justice, Remarks at Ethics and Compliance Initiative Annual Conference (April 24, 2017).

organizations of crimes.[2] Yet in nearly half of these cases, no individuals related to the organization were prosecuted.[3]

The primary goals of all prosecutions of economic crimes are accountability and deterrence. "White collar crime undermines the rule of law, defrauds victims, and disrupts the marketplace."[4] The Department has long recognized that deterrence of corporate crime is most effective when enforcement is consistent and when individuals are brought to account for their specific acts of wrongdoing. As former Attorney General Holder observed, "[f]ew things discourage criminal activity at a firm—or incentivize changes in corporate behavior—like the prospect of individual decision-makers being held accountable."[5] Deterrence is most effective under two conditions: (1) when there is individual accountability; and (2) when there is uniform enforcement of the rule of law.

Prosecution of corporations and other business organizations developed in part as a reaction to the difficulties arising from holding specific individuals accountable for their collective misdeeds, and such prosecutions remain appropriate in many circumstances. But overreliance on these types of prosecutions can become a crutch to avoid the tough work of investigating and prosecuting specific individuals. Moreover, the reality today is that most prosecutions, including prosecutions of corporations, lead to plea agreements and settlements. Corporate settlements in the past have often been perceived as little more than cash buyouts of individual immunity that end up hurting innocent employees and investors.[6] They may also create the further perception that current prosecutors are either too inexperienced or lack sufficient resources to bring to justice responsible individuals. Viewed in this light, corporate settlements may do little to deter future individual misconduct.

---

[2] *Organizations Receiving Fines or Restitution by Primary Offense Category: Fiscal Year 2016*, U.S. SENTENCING COMM'N (2016).

[3] Rod Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, Keynote Address at New York University School of Law on Corporate Enforcement Policy (Oct. 6, 2017).

[4] Rod Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, Remarks at the Bloomberg Law and Leadership Forum in New York (May 23, 2018).

[5] Eric Holder, Att'y Gen., U.S. Dep't of Justice, Remarks on Financial Fraud Prosecutions at New York University School of Law (Sept. 17, 2014).

[6] Rosenstein, *supra* note 3 (discussing how practice of settling with corporations "created the appearance that personal immunity could be exchanged for corporate cash").

Similarly, a lack of clear consistency in enforcing the law, or a lack of just punishment for the individuals within companies who actually caused misconduct, may cause law-abiding corporations and the individuals who run them to feel disadvantaged.[7] Overall, the goal of corporate fraud prosecutions must always be to protect the victims of fraudulent conduct, including not only individuals and companies who suffer direct monetary losses from misconduct but also competitors or fair-minded business rivals who wish to play on a level field.[8]

For these reasons, all prosecutors should approach corporate investigations from the beginning with the same overriding focus on individual accountability. The key question to ask remains: "Who made the decision to set the company on a course of criminal conduct?"[9]

III. Roadblocks to individual accountability

Of course, stating the question is easier than answering it. Many roadblocks can prevent prosecutors from discovering which individual or individuals are truly responsible for a business's criminal acts. Even when the perpetrators' identities are known, problems of proof can persist. While no article can attempt to catalog all problems that can arise in prosecuting an individual as part of a corporate criminal investigation, certain common themes tend to emerge.

One common problem is the fact that the corporation itself is typically a target or at least a subject of potential criminal charges. Corporations in some respects have interests similar to other targets and potential individual defendants. Just as individuals are often loyal to the companies they serve, so too is the corporation's first interest and loyalty often toward the individuals who effectively decide the corporation's actions. A corporate criminal, like an individual criminal, may require strong incentives to cooperate with the government. Some corporations have in the past expressed unwillingness to cooperate absent individual carve-outs. At minimum, corporations may seek certainty and specificity as to the likely

---

[7] *Id.*

[8] Matthew Miner, Deputy Assistant Att'y Gen., U.S. Dep't of Justice, Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption compliance in High Risk Markets (July 25, 2018).

[9] Rosenstein, *supra* note 3.

resolution of individual charges and may well prefer a global or interlocking settlement.

In other respects, corporations are nothing like a typical individual defendant. Corporations can have financial assets that vastly exceed nearly all individuals. They are owned by others. Those owners could be anyone from inside individuals (who may themselves be targets) to innocent outsiders. For companies that are publicly traded in particular, their public image is itself a goodwill asset. Such companies may have a particular interest in a quick and complete resolution of investigations to avoid battering that image through a long and drawn-out federal investigation and to allow the company to move beyond the problem. The company's goal of reaching a quick and complete resolution, however, is sometimes at odds with prosecutors' goal of a thorough investigation that aims to hold individuals accountable; this is particularly true when the charges against individuals are likely to drag out the bad will afforded the company and its owners. In light of these unique characteristics of corporate defendants and investigations, prosecutors must strongly "consider the impact on innocent employees, customers, and investors who seek to resolve problems and move on."[10] Excessive and unfocused penalties imposed on corporations can "harm innocent shareholders, employees, and other stakeholders."[11]

As a final point, the transnational reach of many corporations presents further impediments to the effective enforcement of this nation's federal criminal laws. Cross-border investigations can present particularly thorny issues due to the limits that exist on information-sharing between nations.[12] Discovery may be impossible and, when it occurs at all, may require coordination with the Office of International Affairs or the State Department, which may delay swift resolution of an investigation. Even when prosecutors can successfully identify the individuals responsible for specific corporate misdeeds and amass sufficient proof to justify criminal charges, the identified defendants may escape justice if they are foreign nationals living outside the United States. For example, the government recently charged several corporate leaders of Volkswagen with fraud, but

[10] Rod Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, Remarks at the American Conference Institute's 20th Anniversary New York Conference on the Foreign Corrupt Practices Act (May 9, 2018).
[11] Miner, *supra* note 8.
[12] Rosenstein, *supra* note 10.

Germany will not extradite its civilian leaders to face trial in America.[13]

Corporate investigations also face many of the same problems that are typical of individual fraud investigations, as well as white collar criminal cases more generally. Lower level employees may have made poor decisions or engaged in plainly negligent acts. Yet, it may still be difficult to prove an actual intent to defraud or even knowledge that the acts in question were criminal. Low-level employees may claim they were simply following orders from above. If those higher-level employees cannot be identified or targeted, outside observers may argue that the Department is simply scapegoating without getting to the true root of the problem.

On the flipside, managers or even owners of companies may have engaged in clearly negligent supervision but may, in fact, have been unaware of criminal conduct of those below them. In some cases these high-level leaders may paint themselves as disengaged or nearly totally removed from the day-to-day decisions that landed the company in hot water. Alternatively, managers or leaders aware of misconduct may have disclosed their actions to others and received advice from counsel that their actions were legally permissible. In all of these instances, it may not be possible to identify the decision-maker who truly set the company on the course of criminal conduct, or it may be clear that the criminal activity stemmed from the group activities of the corporation as a whole, rather than any one individual. Instead, prosecutors may be left able only to pursue actions solely against the corporation itself under the collective knowledge doctrine.[14]

Even when prosecutors successfully identify the relevant decision-maker, there will often be little direct evidence establishing intent, which is frequently the key factual question at issue in fraud cases. Senior executives often avoid using email or otherwise creating documentary smoking guns that show direct knowledge of fraud.[15] Instead, prosecutors must themselves infer, and at trial hope jurors will infer, intent from circumstantial evidence. Cooperating witnesses may fill in gaps or provide direct evidence, but this evidence will carry

---

[13] Peter J. Henning, *Why It Is Getting Harder to Prosecute Executives for Corporate Misconduct*, 41 VT. L. REV. 503, 509 (2017).

[14] United States v. Bank of New England, N.A., 821 F.2d 844, 856 (1st Cir. 1987).

[15] Michael S. Schmidt & Edward Wyatt, *Corporate Fraud Cases Often Spare Individuals*, N.Y. TIMES, Aug. 7, 2012.

the same baggage that always accompanies government cooperators and will rarely suffice to carry the day alone.

IV. The Yates Memo principles

While problematic, the above difficulties are not insurmountable in many cases. As always, the Department's goal is "to enhance the predictability and consistency of the law."[16] Such predictability, and deterrence as a whole, are best achieved when legal principles are clearly known and consistently applied.

The Department has issued guidance to prosecutors aimed at holding individuals accountable for their roles in corporate crime. In September 2015, the Department issued a memorandum, since incorporated into the Justice Manual, setting forth six basic guiding principles.

First, corporations who wish to cooperate in criminal investigations must provide the Department with all relevant facts about the individuals who were involved in corporate misconduct.[17] This principle goes beyond mere admission that the corporation is responsible for misdeeds and requires specific and timely disclosure of the identities and actions of the individuals responsible. It is thus less akin to acceptance of responsibility and more akin to the requirements necessary in the criminal system for relief of mandatory minimum sentences: full and timely disclosure of all information the defendant (here the corporation) has "concerning the offense or offenses that were part of the same course of conduct or of a common scheme or plan."[18]

Second, prosecutors should focus on individual wrongdoers from the earliest stages of the investigation.[19] Rather than simply focusing on the big picture actions of the corporation, investigators should zero in on individual targets. This early focus on individuals can guide the direction of the investigation. Moreover, as prosecutors amass evidence against individual targets, they can encourage those individuals to cooperate against others (or against the corporation),

---

[16] Rosenstein, *supra* note 4.

[17] Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, Individual Accountability for Corporate Wrongdoing 3 (Sept. 9, 2015) [hereinafter Yates Memo].

[18] U.S. SENTENCING GUIDELINES MANUAL § 5C1.2(a)(5) (U.S. SENTENCING COMM'N 2004).

[19] Yates Memo, *supra* note 17, at 4.

which increases the likelihood of developing a case against the most culpable corporate leaders.

Third, criminal prosecutors should coordinate with their civil counterparts and institute parallel proceedings where appropriate (but without piling on).[20] The goal should always be to most effectively hold individuals responsible. At times, there may be too many roadblocks to criminal prosecution, but declination need not mean that individuals get off scot free. The civil system can provide a host of remedies, including financial penalties on individuals (monetary damages, restitution, disgorgement, forfeiture), as well as personal sanctions like suspension or debarment.

Fourth, absent extraordinary circumstances or specific Department-approved policies, prosecutors may not agree to absolve individuals of wrongdoing.[21] Corporations act through individuals, and there is significant evidence that deterrence is best achieved through taking action against individuals.

Fifth, prosecutors should work diligently to resolve parallel individual and corporate cases within the statute of limitations.[22] Tolling agreements should be minimized. In general, prosecutors should not resolve cases against entities prior to charging all related individuals, or concluding that declination is appropriate.

Sixth, civil attorneys should consider factors beyond an individual's current ability to pay when deciding whether to file suit.[23] Among the important relevant factors are the seriousness of the person's misconduct and the importance of the federal interest. Even if the case is unlikely to provide significant monetary return, pursuing civil individual actions can provide significant long-term deterrence and send an important message to victims and the communities that the Department serves.

V. Strategies for success

By following these principles and considering the Department's overriding focus on accountability and deterrence in the pursuit of justice, government attorneys can overcome many of the common roadblocks to a successful criminal prosecution or individual civil enforcement action. Several common themes emerge.

---

[20] *Id.*

[21] *Id.* at 5.

[22] *Id.* at 6.

[23] *Id.*

First, prosecutors at the very beginning stages of any investigation must clearly identify individual targets and create a focused plan for determining whether criminal charges are viable against those targets. Identifying a plan of attack leads to speedier resolution of cases and investigations.[24] This clarity has the added benefit of making it easier for corporate defense counsel to advise clients and encouraging fuller and earlier cooperation (or make it abundantly clear that no such cooperation is forthcoming).

Second, in formulating an investigative plan, prosecutors should carefully consider how covert or overt the investigation should be. Covert investigations require significant advance planning and typically cannot remain under wraps for long. Identify likely defenses and plan interview questions well in advance to pin down witnesses and determine the viability of defenses, such as lack of intent or advice of counsel.

Third, once the investigation is actively overt, make all efforts to enlist corporate counsel as an ally. While investigation of corporate crime is an inherently adversarial process, the Department recognizes and rewards companies that work in good faith to help uncover crimes and deter future misconduct.[25] It is unsurprising that within large, and often transnational, corporations there "can exist one or a few bad apples," some of whom may have been inherited through acquisitions or decisions of prior leadership teams.[26] Sometimes when corporations themselves take clear actions to hold individuals accountable, the interests of justice are best served through declination rather than pursuit of additional charges against either individuals or the corporation. For example, the Department recently declined to prosecute Dun & Bradstreet after they terminated and disciplined employees of a Chinese subsidiary who engaged in significant corrupt practices.[27] Encouraging such corporate compliance can promote good governance while still accomplishing the government's principal goal of deterring wrongdoing and ensuring legal compliance by corporations and other rational marketplace actors.[28]

Prosecutors should insist that corporate counsel take reasonable good faith steps to provide all relevant information they can compile

---

[24] Miner, *supra* note 8.

[25] Rosenstein, *supra* note 4 (discussing first corporate declination under the Department's new Foreign Corrupt Practices policy).

[26] Miner, *supra* note 8.

[27] *Id.*

[28] Rosenstein, *supra* note 3.

regarding the individuals responsible for misconduct. If corporate counsel are truly not forthcoming, prosecutors must be willing to stand firm and deny acceptance credit to the corporation, while at the same time emphasizing that cooperation can lead to the speedier resolution of charges most corporations ardently desire.

On the other hand, it is important that prosecutors recognize that Department policy only requires truthful disclosure of all known information. Corporations lack many of the tools at the disposal of the Department, including the ability to compel document production and live testimony through grand jury subpoenas. "While a corporate defense lawyer can read email and talk to employees who consent to be interviewed, it should not come as a surprise that corporations and their counsel cannot always crack the case the way that a determined and methodical prosecutor could using the tools at his or her disposal."[29]

Fourth, it is important to keep in mind that most corporate fraud cases involve multiple actors. Like other more traditional conspiracies, it may be necessary to work up the chain. To acquire proof against the ultimate decision-maker, prosecutors may need to level charges against more mid-level or low-level corporate players, consistent with principles of federal prosecution. Immunity should not be granted to individuals, particularly individual decision-makers absent truly extraordinary circumstances and documented approval of the United States Attorney or Assistant Attorney General.[30]

Fifth, prosecutors should take advantage of all legal tools at their disposal in working to build a case. *Pinkerton* instructions are particularly useful in corporate conspiracy cases, because they allow decision-makers to be held responsible for the reasonably foreseeable actions of their subordinates.[31] Instructions discussing the narrowness of an advice of counsel (or "good faith") defense can demonstrate that a

---

[29] Barry H. Burke & Paul H. Schoeman, *DOJ Policies on Corporate and Individual Prosecutions Should Be Reconsidered, Recalibrated*, N.Y. LAW. J., Dec. 11, 2017.

[30] Yates Memo, *supra* note 17, at 5.

[31] *See, e.g.*, United States v. Sullivan, 522 F.3d 967, 977 (9th Cir. 2008) (upholding advertising agency CEO's fraudulent concealment conviction based on *Pinkerton* theory).

defendant did not fully disclose all relevant facts or did not actually follow and rely on the lawyer's advice.[32]

Finally, criminal prosecutors should always remember that holding an individual fully accountable for corporate misdeeds is not necessarily synonymous with securing a federal conviction. The path to misconduct may have been set on course by a decision-maker whose culpability cannot be proven beyond a reasonable doubt in federal court. Nevertheless, that individual might be adjudged culpable under a lesser standard of proof. In those cases, parallel civil proceedings may be preferable. Engaging civil attorneys in the United States Attorney community, Main Justice, or an appropriate agency early in a case can ensure that appropriate charges are timely pursued. Coordination in this context is key to ensure that the government does not wind up imposing multiple penalties for the same conduct.[33]

In instances where defendants are beyond the reach of American law, prosecutors should coordinate with their foreign counterparts to determine whether appropriate criminal or civil penalties may be brought under the laws of another nation.[34] State charges or civil suits may also be appropriate if further investigation suggests the federal interest in a particular case is attenuated.

This final point hearkens back to the first point noted: preparing an early plan, thinking through potential defenses, and working quickly can ensure that relevant statutes of limitation do not run out. It also allows for all angles to be considered, which potentially ensures that individuals who commit or assist in corporate crimes are punished. Similarly, bringing in these additional partners can do even more to deter future misconduct and ensure the public and company stakeholders that the Department of Justice (and these other actors) will work to enforce a level playing field and employ all of its resources to vigorously prosecuting corporate fraud.

About the Authors

Thomas L. Kirsch II is the United States Attorney for the Northern District of Indiana and Vice Chair of the White Collar Fraud Subcommittee of the Attorney General's Advisory Committee. Prior to

[32] *See, e.g.*, United States v. Lindo, 18 F.3d 353, 356 (6th Cir. 1994) (laying out the defense); United States v. Philpot, 733 F.3d 734, 747 (7th Cir. 2013) (noting that advice of counsel is a specific form of the good faith defense).
[33] Rosenstein, *supra* note 10.
[34] Miner, *supra* note 8.

his appointment in 2017, Kirsch was a partner at Winston & Strawn LLP in Chicago, focusing his practice on complex commercial litigation, white collar criminal defense, and government investigations. Kirsch has also served the Department as an Assistant United States Attorney and as Counsel to the Assistant Attorney General in the Office of Legal Policy. Kirsch is a Fellow of the American College of Trial Lawyers. He earned his J.D. from Harvard Law School.

David E. Hollar is the Appellate Division Chief for the Northern District of Indiana. A former law clerk to Seventh Circuit Judge Diane P. Wood, he joined the Department of Justice in 2002, where he has also served as a trial Assistant United States Attorney in the Northern District of Indiana and as an attorney in the Criminal Division, Appellate Section. He earned his J.D. from the University of Chicago.

Page Intentionally Left Blank

Parallel Proceedings in Health Care Fraud

Benjamin Greenberg
First Assistant United States Attorney
Southern District of Florida

Susan Torres
Deputy Chief, Civil Division
Southern District of Florida

I. Parallel proceedings are more critical than ever in combatting the complex health care fraud schemes of today

Health care fraud schemes in recent years have become more sophisticated as defendants realize they can no longer get away with the more blatant and easily detected fraud of earlier years. As a result, we increasingly find health care fraud in the context of existing and ongoing businesses, including hospital systems, pharmacies, and nursing homes, that continue to operate and serve patients during and after the government takes enforcement action to address and root out the fraud. These types of cases make the use of parallel proceedings more necessary and vital than ever. Parallel proceedings provide the government with the ability to choose from a broad array of enforcement tools, which can be used separately or in conjunction to fully vindicate the public interest. This vindication can occur, among other ways, by returning fraudulently obtained funds to the public fisc, punishing both individual and corporate wrongdoers, and implementing measures to secure future compliance by the providers at issue.

In South Florida, often referred to as ground zero for health care fraud in America, health care fraud schemes traditionally involved providers whose so-called businesses were entirely comprised of fraud, such as durable medical equipment (DME) providers selling unneeded power wheelchairs. These businesses would close up shop after making millions in a short period of time or as soon as the government started asking questions. The business and the millions it generated would be gone, leaving the government only the option of criminal prosecution—if one of the perpetrators could be found. With the creation of the Medicare Fraud Strike Force in Miami in 2007, the

government made significant inroads into DME fraud, and in subsequent years, against fraud in other areas, such as in the provision of mental health services, physical therapy, and home health. Due to these aggressive enforcement actions, criminals turned to more creative and sophisticated fraud schemes. As just one example, we now often see skilled nursing homes that legitimately provide rehabilitation therapy to their residents but upcode those claims to secure the highest reimbursement possible even though patients do not need the most intense level of therapy. These schemes are more difficult to detect and harder to prove, depending on the specifics of a particular case, they require the government to employ a variety of criminal, civil, and administrative tools. Increasingly, these remedies are being considered in parallel in the health care fraud context to ensure that the right remedy, or the right mix of remedies, is deployed in complex cases.

These types of health care fraud cases are ideally suited to parallel proceedings for at least two reasons. First, the same conduct—for example, paying kickbacks to secure health care referrals—can form the basis of a variety of government actions: a civil claim under the False Claims Act, a criminal charge of health care fraud, or an administrative action for exclusion from participation in federal health care programs. Thus, rather than multiple attorneys, agents, and agencies investigating the same conduct separately, coordinating investigatory resources and avoiding duplication of work makes more sense. Second, parallel proceedings allow the government to pursue different remedies that are critical in the fight against health care fraud. Criminal prosecution ensures individual accountability and significantly furthers deterrence objectives. Civil prosecution under the False Claims Act recovers funds stolen from federal health care programs that serve the elderly and others in need and imposes high financial costs on defendants through multipliers and penalties, which also deters future misconduct. Finally, administrative enforcement can remove the worst offenders from the system altogether by denying them the ability to bill any federal health care programs; it can also impose penalties in certain cases where the False Claims Act is not the best route to address the conduct at issue.

Consider a nursing home engaged in extensive billing fraud. While the government is keenly interested in putting an end to the fraudulent billing, it also must prioritize the needs of the elderly population being cared for in the home and consider what other treatment options, if any, may exist for them in the local community.

A combination of remedies may therefore be appropriate, such as an administrative partial payment suspension to mitigate the losses, criminal investigation and prosecution of the individuals responsible for the scheme and a civil investigation and lawsuit under the False Claims Act to recover monies paid by Medicare due to the fraud, plus penalties. An administratively imposed corporate integrity agreement may also be needed to ensure that the nursing home continues to operate with appropriate oversight and compliance measures so that the fraud is not repeated.

II. How to conduct parallel proceedings

The rise in parallel proceedings has spurred an increased focus on the manner in which such investigations are conducted. More and more, individual and corporate defendants are seeking to have evidence suppressed or charges dismissed based on a variety of constitutional challenges. The claim most often arises when a criminal defendant argues that his Fifth Amendment right against self-incrimination has been violated because evidence obtained in a parallel civil case or investigation was used against him in a criminal case.[1] Requests to sanction the government because an attorney misrepresented the existence or status of a criminal investigation, allegedly in an effort to induce the defendant to provide incriminatory statements for use in the criminal case, are also common. In both scenarios, challenges to the operation of parallel investigations are on the rise. However, this increased level of scrutiny does not mean that Assistant United States Attorneys should be afraid of concurrent or consecutive criminal and civil investigations of the same criminal conduct. Rather, armed with an awareness of the case law and a strict adherence to the high ethical standards incumbent upon any Department attorney, Assistant United States Attorneys can protect themselves from common pitfalls and confidently use parallel proceedings to obtain the most comprehensive and just result for victims of criminal and civil fraud.

Part of the debate and confusion surrounding parallel proceedings arises from the fact that the term "parallel proceedings" is really a misnomer. While the phrase has become shorthand for describing civil and criminal investigations into the same conduct, it has also caused a

[1] The inverse claim—that the government obtained evidence in a criminal case and then improperly used that evidence in a civil case—arises less frequently.

significant degree of confusion. Indeed, the phrase implies that the civil investigation and the criminal investigation must not overlap at all, a proposition that runs contrary to law and Department policy. Parallel lines never intersect, no matter how long or short they are, and the imagery of two parallel lines creates the incorrect impression that the criminal and civil investigations must remain completely and forever separate in terms of intake, sharing evidence, developing strategies, and reaching global resolutions. Before discussing the two most common ways in which government lawyers run afoul of the general rule that courts will not impede parallel proceedings, it is important to note that courts have clearly countenanced the government's right to pursue parallel investigations. In *United States v. Kordel*, the Supreme Court explicitly approved of the government's interest in pursuing both criminal and civil remedies based on the same course of conduct and involving the same individuals and entities.[2] The fact that parallel proceedings often involve criminal and civil investigations into virtually identical conduct is not problematic. Rather, that is the point of the parallel proceedings.

In addition to expressly acknowledging the government's interest and right to seek redress through both civil and criminal avenues, several courts of appeal have been unwilling to inhibit these investigations absent the rare situations discussed below. The D.C. Circuit, in *Securities and Exchange Commission v. Dresser Industries,* explicitly approved of such parallel investigations, noting that "[e]ffective enforcement of the securities laws requires that the SEC and Justice be able to investigate possible violations simultaneously."[3] The court also suggested that absent unusual circumstances, it would give significant latitude and deference to the government in cases in which there are parallel proceedings.[4] This latitude includes not only the decision to initiate parallel proceedings in the first place but also the manner in which the investigations are conducted.[5] Specifically, *Dresser* stands for the proposition that courts "should not block parallel investigations by these agencies in the absence of 'special circumstances' in which the nature of the proceedings demonstrably

[2] United States v. Kordel, 397 U.S. 1, 11 (1970).
[3] Securities & Exch. Comm'n v. Dresser Indus., Inc., 628 F.2d 1368, 1377 (D.C. Cir. 1980).
[4] *See id.* at 1376–77.
[5] *See id.*

prejudices substantial rights of the investigated party or of the government."[6] Though *Dresser* addressed parallel SEC and Department of Justice proceedings, courts have taken a similar approach in cases involving parallel proceedings within the Department of Justice and between Department of Justice and other civil or regulatory agencies. It is therefore critical to appreciate what type of "special circumstances" are likely to result in the suppression of evidence or the dismissal of a case.

A. No affirmative misrepresentations

The first area where courts have been willing to sanction the government is when there is evidence that a government official has affirmatively and intentionally misled the subject of parallel civil and criminal investigations "into believing that the investigation is exclusively civil in nature and will not lead to criminal charges."[7] Most commonly, the defendant in the criminal case claims that the government misled him about the existence of the criminal investigation and induced him to make statements or provide self-incriminating evidence that he would not have provided had he been aware of the criminal investigation. Courts analyze such claims under the Fourth and Fifth Amendments, and generally decline to dismiss cases or suppress evidence in the absence of fraud, trickery, deceit, or a misrepresentation.

United States v. Stringer was a criminal securities fraud case based almost entirely on the same conduct underlying a partially concurrent SEC civil investigation.[8] Before the criminal investigation into the defendants' conduct, the SEC began investigating the defendants and their company for potential civil securities fraud violations based on records falsification and other fraudulent accounting entries.[9] Shortly after the SEC began its investigation, lawyers from the SEC met with lawyers from the United States Attorney's Office to talk about opening a criminal investigation.[10] Over the next year, the SEC the United States Attorney's Office met several times to discuss the coordination of the investigations. Among other things, at the

---

[6] *Id.* at 1377 (citing *Kordel*, 397 U.S. at 11–13).
[7] United States v. Robson, 477 F.2d 13, 18 (9th Cir. 1973).
[8] United States v. Stringer, 408 F. Supp. 2d 1083 (D. Or. 2006), *rev'd in part*, *vacated in part*, 521 F.3d 1189 (9th Cir. 2008).
[9] *See id.* at 1085.
[10] *See id.*

United States Attorney's Office's request, the SEC did not disclose the existence of the criminal investigation to the defendants while taking their deposition. The SEC agreed to depose the criminal targets in a manner that would create the best possible record for false statement charges arising from answers during the deposition, and the SEC asked a court reporter not to tell opposing counsel that there was an Assistant United States Attorney assigned to the case.[11]

Alleging that their Fifth Amendment rights had been violated by the United States Attorney's Office's use of evidence obtained by the SEC, defendants filed motions to dismiss the indictment, or in the alternative, to suppress testimony the SEC had obtained in the civil proceeding.[12] The district court concurred, in part, because while the government had not engaged in deceit, trickery, and intentional misrepresentation by failing to reveal the existence of the active criminal investigation, the government's response to a specific inquiry by one of the defendant's lawyers about the existence or status of a criminal case "was evasive and misleading, particularly in light of the close association between the USAO and the SEC throughout the investigation and the early identification of Stringer as a criminal target."[13]

The Ninth Circuit reversed *Stringer* and agreed with the government that it had no legal obligation to advise the defendants about the existence of a criminal investigation.[14] This was especially true because the defendants were given an SEC Form 1662, which clearly stated that evidence obtained in the civil investigation could be used in a criminal prosecution.[15] The court's decision turned on the fact that the government had not given the defendants false information. Though the SEC lawyers did not tell the defendants that there was an ongoing criminal investigation, such disclosure was not required as long as there were no affirmative misrepresentations. In fact, the Ninth Circuit explicitly noted that "[t]here was no deceit; rather, at most, there was a government decision not to conduct the criminal investigation openly, a decision we hold the government was free to make."[16] In other words, the government is free to keep the

[11] *Id.*
[12] *Id.*
[13] *Id.* at 1089.
[14] *Stringer*, 535 F.3d at 937.
[15] *Id.*
[16] *Id.* at 933.

existence of the criminal investigation secret, but it is obviously not free to make misstatements about the existence of an investigation.

Though *Kordel* was decided almost 50 years ago and is a very short opinion, the Supreme Court has not had an occasion to address these issues in greater depth since that time. It is clear, and not terribly surprising, that an affirmative misrepresentation will likely result in the exclusion of evidence or even the dismissal of counts. Equally clear is that in the absence of such misrepresentations, courts are extremely reluctant to find any misconduct on the part of the government.

B. You cannot use the civil case as a "stalking horse" to obtain an advantage in the criminal case

The most common claim made by defendants is that the government is conducting a civil investigation designed to obtain evidence that will be used in a contemporaneous or future criminal case. These cases, often described as "stalking horse" claims, generally involve accusations that some civil process, such as depositions, interrogatories, or civil investigative demands, are being used for one of two reasons: either because the same evidence cannot be obtained through criminal process or because the government wishes to hide the criminal investigation lurking in the background.

The Supreme Court rejected a "stalking horse" claim in *Kordel,* which held that a defendant may be entitled to a remedy if he can show that "the Government has brought a civil action *solely* to obtain evidence for its criminal prosecution[.]"[17] Ten years after *Kordel*, the D.C. Circuit, in *Dresser*, considered the corporate defendant's motion to quash an SEC administrative subpoena on the grounds that it was issued in bad faith by the SEC in order to further a parallel criminal investigation.[18] Among other things, the court noted that there were clearly legitimate and separate administrative and criminal goals; also the evidence established that the SEC was acting independently from the criminal investigation and otherwise in good faith. The court further held:

> A bad faith investigation, in the Court's conception, is one conducted *solely* for criminal enforcement purposes. Where the agency has a legitimate noncriminal purpose

[17] United States v. Kordel, 397 U.S. 1, 11 (1970) (emphasis added).
[18] Securities & Exch. Comm'n v. Dresser Indus., Inc., 628 F.2d 1368, 1371 (D.C. Cir. 1980).

> for the investigation, it acts in good faith . . . even if it might use the information gained in the investigation for criminal enforcement purposes as well. In the present case the SEC plainly has a legitimate noncriminal purpose for its investigation of Dresser. It follows that the investigation is in good faith, in the absence of complicating factors. There is, therefore, no reason to impose a protective order. . . .[19]

As cases like *Kordel*, *Dresser*, and *Stringer* make clear, appellate courts have given the government significant latitude in the conduct of parallel investigations in the absence of affirmative misrepresentations or evidence suggesting the civil case exists solely to further the criminal investigation.

Because cases are highly fact specific, it is difficult to know exactly when and where a court will draw the line between permissible interaction between criminal and civil investigators and an interaction that crosses the line. In general, courts have been satisfied that the government is acting in good faith as long as criminal prosecutors and agents do not appear to be directing the civil case and the decision-making process on the civil side is independent of any direction from those leading the criminal case.[20]

---

[19] *Id.* at 1387 (internal citations omitted; emphasis added).

[20] *See, e.g.*, United States v. Setser, 568 F.3d 482, 491–93 (5th Cir. 2009) (finding no Fourth Amendment violation when receiver provided records to law enforcement obtained during an SEC investigation of Ponzi scheme because the receiver validly took possession of records and became their lawful custodian); United States v. Posada Carriles, 541 F.3d 344, 366 (5th Cir. 2008) (reversing district court's finding of government misconduct because questions asked of the defendant as part of a naturalization interview were within the scope and subject matter of agent's assigned responsibility); United States v. Greve, 490 F.3d 566, 571–72 (7th Cir. 2007) (finding no Fourth or Fifth Amendment violation because there was no deception on the part of the IRS agent); United States v. Blocker, 104 F.3d 720, 725–30 (5th Cir. 1997) (finding no Fourth Amendment violation where state regulator wore a recording device at FBI direction because the auditor had independent legal access to the subject records and the FBI and United States Attorney's Office had repeatedly instructed auditor to do "nothing more, nothing less and nothing different" than what auditor would otherwise have done); United States v. Copple, 827 F.2d 1182, 1190 (8th Cir. 1987) (finding that there was no violation because the FBI developed evidence through its own investigation that was independent of the FDIC);

III. Practical considerations in parallel proceedings: Department of Justice policy and best practices

Department policy on parallel proceedings is longstanding and well established in memorandums spanning more than three decades.[21] All of these directives mandate that United States Attorneys' Offices have policies and procedures in place for the coordination of parallel proceedings. While specific practice in this area may vary from district to district, the overarching goal is the same—criminal and civil attorneys and their agency counterparts should communicate, coordinate, and cooperate on a timely basis "to the fullest extent appropriate and permissible by law."[22] The Holder Memo highlighted white collar cases as particularly appropriate for parallel proceedings,

---

United States v. Okwumabua, 828 F.2d 950, 953 (2d Cir. 1987) (affirming district court's decision denying motion to suppress admissions because agent did not affirmatively mislead defendant); United States v. Unruh, 855 F.2d 1363, 1374 (9th Cir. 1987) (affirming denial of motion to dismiss because there was no evidence that the civil case was brought in bad faith); United States v. Mahaffy, 446 F. Supp. 2d 115, 126 (E.D.N.Y. 2006) (holding that district court properly denied the motion to suppress statements to SEC investigators because the civil investigation was separate enough from the parallel criminal investigation, the targets knew of the criminal investigation, and "[t]here are no facts to suggest that the USAO hid behind or manipulated the S.E.C. with the intention of misrepresenting its true intentions to the defendants"); United States v. Teyibo, 877 F. Supp. 846, 856 (S.D.N.Y. 1995), *aff'd*, 101 F.3d 681 (2d Cir. 1996) (denying the defendant's motion to suppress evidence in criminal case because the "SEC pursued its own independent investigation of [the defendant's] activities and did not consult with the United States Attorney's office in any substantive way . . . [and] the United States Attorney's Office properly conducted its own investigation and maintained grand jury secrecy as is required by federal law.").

[21] *See* Memorandum from Edwin Meese III, Att'y Gen., U.S. Dep't of Justice, Coordination of Criminal and Civil Fraud, Waste and Abuse Proceedings (July 16, 1986); Memorandum from Janet W. Reno, Att'y Gen., U.S. Dep't of Justice, Coordination of Parallel Criminal, Civil, and Administrative Proceedings (July 28, 1997); Memorandum from Eric H. Holder, Att'y Gen., U.S. Dep't of Justice, Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings (Jan. 30, 2012) [hereinafter Holder Memo].

[22] *See* Holder Memo, *supra* note 21.

and it emphasized that coordination should continue throughout the life of a matter—from intake through resolution.[23]

The more recent Yates Memo on individual accountability in corporate cases reiterated the Department's policy on parallel proceedings and noted that criminal and civil attorneys should reconsider the potential for parallel proceedings or remedies throughout the course of their investigations.[24] This is a critical point because matters that do not at first appear as appropriate for parallel development may become so as the investigation proceeds.

These policies on parallel proceedings are essential in the complex health care fraud cases that are increasingly becoming the norm, and every district should reevaluate its policies periodically to ensure that they adequately address the needs of these types of cases. As a general matter, the following principles and types of activities generally fall within the heartland of accepted practices:

- There need not be, and indeed should not be, a "Chinese wall" between civil investigators/Assistant United States Attorneys and criminal investigators/Assistant United States Attorneys.[25]
- Civil and criminal Assistant United States Attorneys may discuss the evidence against certain targets or subjects as long as they comply with applicable grand jury secrecy rules.
- Overall case strategy and timing can be freely discussed.

In order to avoid any potential problems, Assistant United States Attorneys should be mindful of the following:

- Make sure there is a good faith and articulable, legitimate reason for initiating the civil investigation. This takes away the defendant's argument that the civil investigation was initiated solely for the purpose of obtaining evidence for use in a criminal prosecution. This is important regardless of whether the civil case is initiated before or after the criminal case.
- Criminal Assistant United States Attorneys should refrain from giving direction to civil Assistant United States Attorneys about

---

[23] *Id*.

[24] *See* Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, Individual Accountability for Corporate Wrongdoing 5 (Sept. 9, 2015) [hereinafter Yates Memo].

[25] Such a wall may have to exist as to evidence obtained by grand jury subpoena or from witness testimony before the grand jury. *See* FED. R. CRIM. P. 6.

specific questions to ask in depositions/interrogatories or specific pieces of evidence to gather. The more it appears that the civil Assistant United States Attorneys are taking certain actions at the request of the criminal Assistant United States Attorneys for the benefit of the criminal case, the more likely it is that courts will find that the civil investigation is merely a "stalking horse" for the criminal investigation.

Highlighted below are a few additional best practices for parallel proceedings in complex health care fraud matters.

Intake in Strike Force Cities: Effective coordination may present special challenges in Strike Force cities like Miami. The Strike Force model typically involves quickly developing cases discussed during regular meetings of the Strike Force. This working model does not lend itself to the type of joint intake commonly recommended in matters where parallel proceedings are likely to occur. As a result, it is imperative that criminal prosecutors handling health care fraud cases in a Strike Force city be attuned to the Department's parallel proceedings policy and consistently evaluate their cases for possible referral to civil attorneys or their agency counterparts. Similarly, civil health care fraud qui tam cases should be shared upon receipt with the office's criminal division to determine early on whether a criminal investigation is appropriate. In accordance with the Yates Memo, it is also important for civil attorneys to assess throughout a civil investigation whether evidence that the investigation has uncovered warrants a subsequent review by the criminal division.[26] It may be especially important in Strike Force cities to foster routine communication among attorneys responsible for civil and criminal health care fraud matters, whether by co-locating the units that handle such matters or establishing some other type of periodic coordination.

Seeking documents in parallel cases: In addition to intake issues, Department policy on parallel proceedings discusses how to maximize information-sharing by deferring use of the grand jury process in favor of other methods that do not present secrecy issues. The Holder Memo, however, also notes that "[w]here evidence is obtained by means of a grand jury, prosecutors should consider seeking an order under Federal Rule of Criminal Procedure 6(e) at the earliest appropriate time to permit civil, regulatory, or administrative

[26] *See* Yates Memo, *supra* note 24, at 5.

counterparts access to material[.]"[27] Thus, in districts where criminal prosecutors are more likely to use the grand jury early in an investigation, they should also consider seeking Rule 6(e) orders as soon as it is apparent that a civil investigation is underway. If such an order is obtained, civil and criminal prosecutors should discuss early on what the best methods are for obtaining documentary evidence in health care fraud investigations, which typically involve a high volume of documents. The attorneys may have different standard formats for requesting documents, the scope of the documents sought may be different, and civil attorneys may want to obtain sworn interrogatory responses in addition to documents. This may necessitate the issuance of separate grand jury subpoenas and civil investigative demands, but in either case the issues should be discussed ahead of time.

Warn witnesses. Where both civil and criminal investigations exist, civil attorneys should consider providing all witnesses, and certainly those whose testimony is obtained by civil investigative demand, with appropriate warnings. These warnings could be in writing or on the record during oral testimony pursuant to a Civil Investigative Demand (CID). Either way, they ensure that witnesses are formally on notice that anything they say can subsequently be used in a criminal investigation.

Who goes first? This is increasingly a question out of the hands of Department attorneys. In our district, courts have become more reluctant to stay civil qui tam actions because of pending criminal investigations or prosecutions. This development underscores the need for early coordination so that the criminal side has the opportunity to conduct a thorough investigation prior to the unsealing of the civil action and the disclosures required in civil litigation. With coordination and effective information-sharing, however, both civil and criminal attorneys should be able to employ the appropriate remedies regardless of who goes first.

IV. Achieving a just outcome in parallel proceedings

Parallel proceedings in health care fraud cases often lead to global resolutions, where the criminal, civil, or administrative actions are all jointly brought to conclusion. While the civil resolution should be

[27] *See* Holder Memo, *supra* note 21.

handled by the civil attorneys, and the criminal resolution should be negotiated by the criminal prosecutors, coordination of these remedies into one global agreement is often beneficial to defendants by providing them finality. Recent guidance from Deputy Attorney General Rod Rosenstein reiterates that the goal of such resolutions is "to achieve an equitable result."[28] Such a result requires the same type of coordination that should prevail throughout the course of parallel proceedings to ensure that the public interest is vindicated and that the appropriate enforcement tools are utilized. Rosenstein's memo introduced a new provision in the Justice Manual entitled, "Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct."[29] This section emphasizes Department attorneys' longstanding obligation not to use criminal enforcement as leverage to extract increased civil damages, and it urges coordination "to avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture against [a] company."[30] The section also encourages the same type of coordination with any state, local, or foreign enforcement authorities that are investigating the same misconduct.

Importantly, the Justice Manual provides that "all relevant factors" should be considered in deciding "whether coordination and apportionment . . . allows the interests of justice to be fully vindicated."[31] In health care fraud cases, for example, these factors should include a focus on the defendant's conduct, including the nature and extent of the fraud involved, the amount drained from federal health care programs, and whether the conduct caused patient harm. Conversely, the timeliness and extent of the defendant's cooperation with the Department should also be considered.

This guidance builds upon preexisting parallel proceedings policies that simultaneously advocate for the full use of available remedies against wrongdoers while also encouraging coordination of the various tracks of enforcement activity. The new Justice Manual section on coordination of corporate resolution penalties seeks to strike that same balance, emphasizing fairness in resolutions rather than "piling

---

[28] Memorandum from Rod Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, Policy on Coordination of Corporate Resolution Penalties (May 9, 2018).

[29] JUSTICE MANUAL § 1-12.100.

[30] *Id.*

[31] *Id.*

on" repetitious sanctions for the same conduct while preserving Department attorneys' flexibility to consider additional remedies in appropriate matters.

About the Authors

Susan Torres is an Assistant United States Attorney and Deputy Chief in the Civil Division of the United States Attorney's Office for the Southern District of Florida, where she supervises the Division's ACE matters. Her practice primarily involves prosecuting civil health care fraud cases. She has spoken on pretrial asset restraints and the False Claims Act at the NAC, the Department of Justice's National Health Care Fraud Conference, and at meetings of the ABA, AHLA, Florida Bar, and several other organizations.

Ms. Torres wrote an article in the November 2016 DOJ Journal of Federal Law and Practice, formerly the United States Attorneys' Bulletin, on pretrial asset restraints. It can be found at https://www.justice.gov/usao/page/file/915836/download.

Benjamin Greenberg previously served as the United States Attorney for the Southern District of Florida and as First Assistant United States Attorney from 2010–2017. He previously held a number of leadership positions, including serving as the first Chief of the newly created Special Prosecutions Section, where he oversaw efforts to combat violent crime, child exploitation, and human trafficking. In 2009, Mr. Greenberg became Chief of the Narcotics Section. Mr. Greenberg joined the United States Attorney's Office in 2000 and handled a wide variety of cases, including the prosecution of the President and Chief Executive Officer of a well-known financial institution for securities and bank fraud arising from a complex international accounting fraud scheme.

Recent Trends in Criminal Health Care Fraud Prosecutions

Ranee A. Katzenstein
Assistant United States Attorney
Chief, Major Frauds Section
Central District of California

Diidri Robinson
Former Assistant Chief Criminal Division, Fraud Section
United States Department of Justice

Benjamin Barron
Assistant United States Attorney
Deputy Chief, OCDETF Section
Central District of California

Ashwin Janakiram
Assistant United States Attorney
Central District of California

Alexander F. Porter
Assistant United States Attorney
Central District of California

I. Introduction

Nearly a fifth of the United States' economy is spent on health care. According to the Centers for Medicare & Medicaid Services (CMS), in 2016, personal health care expenditures in the United States were approximately $3.3 trillion, an amount that was roughly 17.9% of GDP.[1] Medicare spending was approximately $672.1 billion of that total, Medicaid spending was approximately $565.5 billion, and spending by private health insurance programs was over $1 trillion.[2] With so much money at stake, it is not surprising that some individuals seek to abuse the health care system to fraudulently enrich themselves. Indeed, experts estimate that tens to hundreds of

[1] CTRS. FOR MEDICARE & MEDICAID SERVS., NATIONAL HEALTH EXPENDITURES 2016 HIGHLIGHTS, at 1 (2016).
[2] *Id.* at 2.

billions of dollars are lost to fraud each year.[3] The importance of addressing this fraud cannot be overstated. Concerted action to reduce fraud causing losses to Medicare, Medicaid, and other public health insurance programs plays an important part in assuring that the government meets its obligation to be a prudent and effective steward of public funds. Preventing fraud and abuse in both the private and public sectors of the industry, thereby helping to keep health care costs down, also serves the public welfare because high cost is the primary reason Americans have given for problems they experience accessing medical care.[4]

Fighting health care fraud has been one of the Department of Justice's priorities for many years. It is a particular priority in the Central District of California (CDCA), where health care spending has continued to increase in recent years. Enforcement efforts in the CDCA are bolstered by the presence of a dedicated Medicare Fraud Strike Force through which the United States Attorney's Office partners with the Department of Justice's Criminal Division (Fraud Section), the Federal Bureau of Investigation (FBI), and the U.S. Department of Health and Human Services Office of the Inspector General (HHS-OIG). Working together, Assistant United States Attorneys, Department of Justice trial attorneys, and FBI and HHS-OIG agents have achieved significant results in prosecution, thereby helping to deter criminal conduct in the health care arena. Among other methods, prosecutors and agents in the CDCA use data analytics to identify potential targets and focus on the most egregious frauds. They have developed innovative charging theories to ensure our ability to address a vast array of frauds that might otherwise escape prosecution. The success of this partnership is reflected in the

---

[3] *See, e.g.*, *The Challenge of Health Care Fraud,* NAT'L HEALTH CARE ANTI-FRAUD ASSOC., https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx (last visited October 8, 2018); *see also* James Byrd, Paige Powell, & Douglas Smith, *Health Care Fraud: An Introduction to a Major Cost Issue*, 14 J. ACCT., ETHICS & PUB. POL'Y (2013) (noting that, in addition to its financial impact, fraud in the health care industry potentially affects individuals' health and lives); Donald M. Berwick, MD, MPP & Andrew D. Hackbarth, MPhil, *Eliminating Waste in US Health Care*, 307 J. AM. MED. ASS'N 1513, 1514 (2012) (estimating that fraud and abuse cost Medicare $98 billion and cost the entire health care system $272 billion).

[4] DEP'T FOR PROF'L EMPS., *The U.S. Health Care System: An International Perspective* (2016).

cases charged in the CDCA as part of this year's National Health Care Fraud Takedown, in which the total cumulative loss alleged is $660 million, approximately 1/3 of the total nationwide.[5]

This article surveys recent trends in the Department's health care fraud prosecutions with a focus on developments in the CDCA as examples of these trends. It is not meant to be comprehensive, but rather to highlight current areas of concern, new schemes that are being used, and approaches that have been successfully taken to address them.

II. Medicare fraud hot spots

As the charts in Figures 1–3 demonstrate, throughout this decade, the CDCA has witnessed a marked increase in Medicare spending in three fraud hot spots: home health, hospice, and Part D.[6] Over the past five years, Medicare spending in these areas has increased by $51.9 billion.[7] While the fraudulent schemes vary, the common trend among these three hot spots is the payment of kickbacks to medical professionals, marketers, and beneficiaries.[8]

---

[5] Press Release, U.S. Dep't of Justice, National Health Care Fraud Takedown Results in Charges Against 601 Individuals Responsible for Over $2 Billion in Fraud Losses (June 28, 2018); Press Release, U.S. Dep't of Justice, As Part of National Healthcare Fraud Sweep, Los Angeles-Based Prosecutors Filed 16 Cases Alleging $660 Million in Fraudulent Bills (June 28, 2018).

[6] Figures provided herein courtesy of HHS-OIG.

[7] CMS One Program Integrity.

[8] The harm from kickbacks in the health care industry goes beyond the financial losses that may be caused. At the sentencing hearing of an administrator who paid kickbacks to doctors for referrals of spinal surgeries to his hospital, the Court stated: "[A] defendant's offering of kickbacks to doctors should be presumed to have its intended effect. That is, the defendant's scheme is of the type that intentionally interferes with the doctor-patient relationship and taints the independent medical decision-making process. Quite simply, defendant introduced greed into the physician-patient relationship. . . . Patients who were steered to the defendant's hospital, particularly those vexed with lasting complications from their spinal surgeries now . . . have the added doubt of whether their kickback-receiving doctors had their best interest in mind in selecting and recommending this particular hospital and this particular surgery." Transcript of Proceedings, United States v. Drobot, No. 8:14-cr-00034-JLS (C.D. Cal. Jan. 12, 2018), ECF No. 134.

A. Home health

Medicare covers the following types of home health services: (1) intermittent skilled nursing or home health aide care; (2) physical therapy; (3) occupational therapy; (4) speech language pathology; and (5) medical social services. In order to receive home health services, a physician must certify that the beneficiary is homebound and place the beneficiary under a plan of care. Medicare payments to home health agencies in the CDCA have steadily increased since 2010 (See Fig. 1). In order to obtain more than their fair share of these payments, fraudulent home health agencies (HHAs) often enter into kickback relationships with medical professionals in order to meet this certification requirement, which allows the HHAs to submit millions of dollars in fraudulent claims to Medicare.

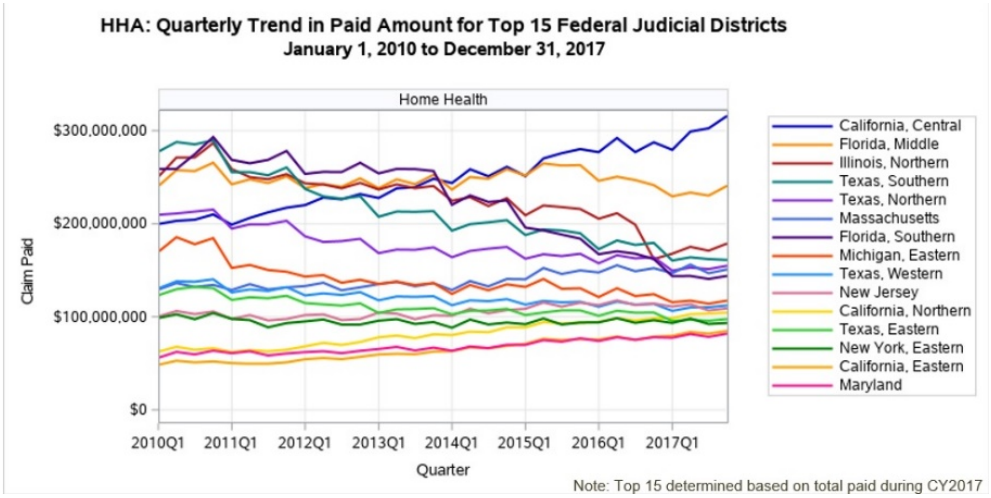

Figure 1. HHA Payment Trends by Federal Judicial District

For example, in the CDCA, a physician assistant (PA) was recently indicted for his role in a multi-million dollar conspiracy to fraudulently bill Medicare for home health services generated by kickback payments.[9] The PA was responsible for evaluating an estimated 4,000 patients for home health care and fraudulently caused Medicare to pay approximately 35 million dollars to HHAs. One of the PA's co-conspirators was a physician who accepted kickback payments in exchange for signing home health certifications

[9] United States v. Filian, No. CR 18-374-JFW (C.D. Cal. 2018) (The defendant pleaded not guilty and, as of this writing, is awaiting trial.).

for beneficiaries examined by the PA.[10] Most of these Medicare beneficiaries were not homebound. Some lived in locations 50–100 miles from the home health agencies' locations in Los Angeles and were recruited to home health care by the promises of free shoes and juice. In exchange for the false certifications to home health care, the PA received payments from at least 18 HHAs amounting to over $1 million in kickbacks. The PA laundered the proceeds of his fraud by creating numerous shell corporations and conducting multiple transactions between various bank accounts.

B. Hospice

Like home health care, Medicare payments for hospice services have also climbed in the CDCA since 2010 (See Fig. 2). In order for a beneficiary to obtain hospice care covered by Medicare Part A, a physician must certify that the beneficiary is terminally ill, meaning that the beneficiary is expected to live for six months or less. As with home health care, this certification requirement serves as the basis of kickback relationships between hospice owners, recruiters, and medical professionals.

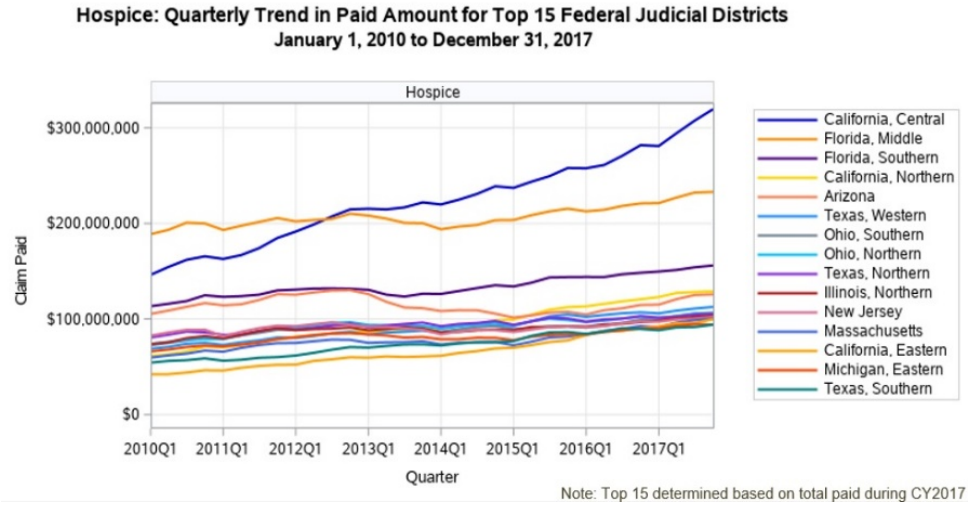

Figure 2. Hospice Payment Trends by Federal Judicial District

Beyond proving a kickback relationship, a key issue in hospice fraud cases centers on whether the physician fraudulently certified that a

[10] United States v. Levine, No. CR 17-126-ODW (C.D. Cal. 2017) (As of this writing, the defendant has pleaded guilty and is awaiting sentencing).

beneficiary was terminally ill. A good indicator of the physician's knowledge and intent is the percentage of the physician's hospice certified patients who survived longer than six months. In a hospice fraud trial in the CDCA, for example, only a small percentage of the hospice facility's patients had died within the projected six-month time frame, and many of the patients who testified at trial were in good health, establishing that they had not and did not require end-of-life care.[11] The evidence at trial showed that the hospice facility's owners paid patient recruiters to bring in Medicare and Medicaid of California (Medi-Cal) beneficiaries to receive "assessments" by nurses. Regardless of the outcome of the assessments, the two physician-defendants certified that the beneficiaries were terminally ill, even though they were not. The fraudulent scheme resulted in the submission of more than $8 million worth of fraudulent bills to Medicare and Medi-Cal. The two physician-defendants were convicted of various health care fraud violations and were sentenced to nine and four years, respectively.

C. Part D

Medicare payments under Part D are also on the rise (See Fig. 3). Unlike other parts of Medicare, Part D is run by private contractors that are paid by the government to process bills. The payment structure and complexity of the Part D programs make them particularly vulnerable to fraud, waste, and abuse, according to reports by CMS, the United States Government Accountability Office, and HHS-OIG. Examples of Part D fraud include pharmacies billing for drugs without a valid prescription or without dispensing the drugs at all, physicians receiving kickbacks and other benefits for prescribing certain medications, physicians filling and then reselling their prescriptions, and licensed medical professionals providing prescriptions for patients they have never seen.

[11] United States v. Wijegoonaratna, et al., No. CR 14-512-SJO (C.D. Cal. 2014).

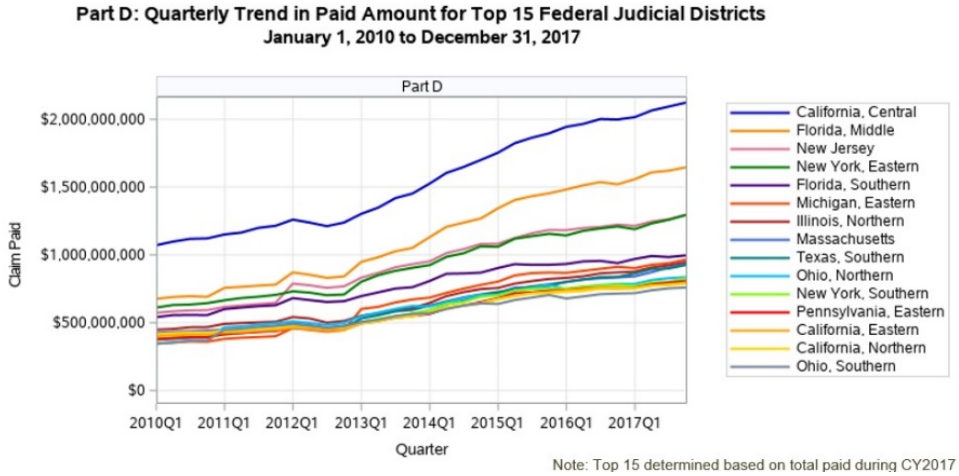

Figure 3. Part D Payment Trends by Federal Judicial District

While the opioid epidemic has certainly contributed to Part D fraud schemes, there are also increasingly more schemes centered on non-controlled substances. This shift can be attributed in part to the belief that there is less government scrutiny of non-controlled substances and the fact that sales of many brand name, non-controlled substances can yield a higher profit margin. Popular non-controlled drugs at the center of many Part D schemes include antipsychotics, cholesterol drugs, respiratory inhalers, and HIV drugs.

A June 2018 indictment in the CDCA alleged multiple health care fraud conspiracies perpetrated by the pharmacist/owner of two pharmacies and her co-conspirators.[12] Between 2014 and 2017, the pharmacist/owner submitted claims to Medicare and Medi-Cal for expensive, brand name prescription drugs, including antipsychotics and respiratory inhalers, which were never dispensed to beneficiaries, but rather were provided to co-conspirators for resale on the black market. In addition to submitting prescription claims for drugs never dispensed and diverting those prescription drugs to the black market, the pharmacist/owner, who was the lead defendant in the case, paid kickbacks to marketers in exchange for patient referrals to her pharmacies. Finally, the pharmacist/owner paid and caused the payment of kickbacks directly to Medicare beneficiaries in exchange for filling their prescriptions at her pharmacies. Between

[12] United States v. Sadovsky, et al., No. CR 18-375-AB (C.D. Cal. 2018) (All defendants pleaded not guilty and, as of this writing, are awaiting trial).

January 2014 and September 2017, Medicare Part D plan sponsors reimbursed the pharmacies $45 million for prescription claims. In the same time period, Medi-Cal reimbursed the pharmacies $9 million for prescription claims.

III. The opioid epidemic's impact on health care fraud

The devastation caused by the opioid epidemic is well known. The Department has implemented a number of initiatives to address this scourge, including community outreach as well as traditional enforcement measures based on prosecutions brought by United States Attorneys' Offices throughout the nation. The following discussion addresses the role that health care fraud investigations and prosecutions can play in efforts to tackle the epidemic.

During the first 15 years of the opioid epidemic, the prescription narcotics primarily sought after on the black market were brand name drugs such as OxyContin, a long-acting form of oxycodone manufactured by Purdue Pharma and first introduced to the wholesale market in 1996. Because of the high cost of OxyContin and other brand name narcotics, health care fraud was an important part of the black market opioid trade. For example, drug dealers and related conspirators would recruit indigent beneficiaries to bill Medicare, Medicaid, and other programs for the cost of filling fraudulent prescriptions and would pay cash kickbacks to the recruited beneficiaries. Large scale opioid suppliers would thus acquire their source of supply using taxpayer funds.

In 2010, Purdue changed the formulation of OxyContin pills, making them harder to crush and thus making it harder for addicts to abuse the drug by snorting or shooting up the contents of the pills.[13] The black market shifted with the change. Drug dealers increasingly sought out generic narcotics, such as short-acting oxycodone rather than OxyContin. Because those generics are markedly cheaper, the black market also largely transitioned to an all cash business. Almost all of the doctors prosecuted for drug diversion in Los Angeles ran such cash businesses. For example, Dr. Daniel Cham recently pled guilty to both drug trafficking and money laundering connected to his narcotic prescribing. To conceal his large scale criminal operation,

[13] Keith Humphreys, *A Drug Company Tried to Make Opioids Harder to Abuse. It Backfired.*, THE WASHINGTON POST, July 10, 2017.

Cham used bank accounts in the names of shell businesses to launder hundreds of thousands of dollars in illicit proceeds. In March 2018, Cham was sentenced to 160 months prison for perpetrating the pill mill scheme.[14]

Likewise, when Drug Enforcement Administration (DEA) agents searched the office of Dr. Edward Ridgill in 2015, they found patient files literally stuffed with cash. (See Photo 1). Ledgers seized from the office showed that Dr. Ridgill charged flat cash fees for every patient, and his bank records showed that he received more than $500,000 in cash proceeds. Dr. Ridgill was recently convicted at trial in Los Angeles on charges of running a narcotic pill mill. The financial evidence played an important part in securing both the conviction and the resulting 60-month prison term.[15]

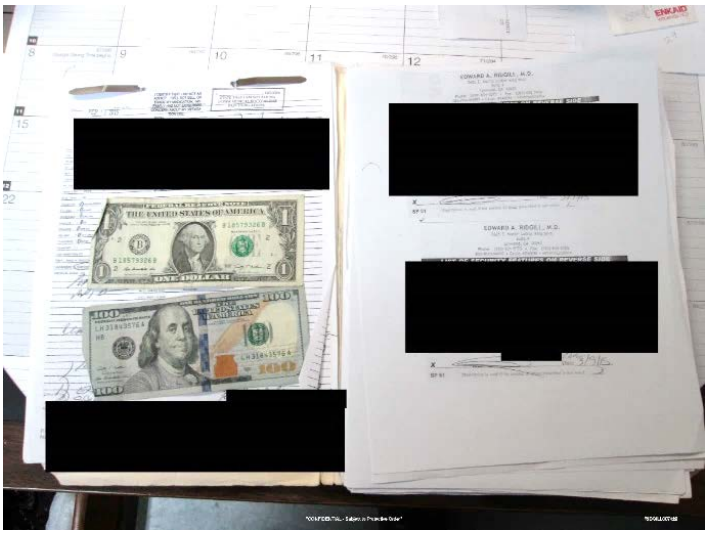

Photo 1: Example of Patient File Found at Dr. Edward Ridgill's Office

Recent cases have also shown that corrupt pharmacies often run cash businesses, which allows them to evade audits and the related oversight that comes with large narcotic billings to Medicare, Medicaid, or other insurers. A jury recently convicted the owners of Global Compounding Pharmacy, brothers Berry and Dalibor Kabov, of using the business as a front for a massive black market narcotics trade.[16] Financial evidence showed that they received no insurance

[14] United States v. Cham, No. CR 14-591-AG (C.D. Cal. 2014).
[15] United States v. Ridgill, No. CR 16-631-SJO (C.D. Cal. 2016).
[16] United States v. Kabov et al., No. CR 15-511-DMG (C.D. Cal. 2015).

proceeds for any of the narcotics they sold. Rather, they received more than $3 million in cash over a period of less than three years, which they spent on private jets, penthouse suites, and other trappings of a lavish lifestyle.

Nevertheless, traditional health care fraud continues to play an important part in opioid diversion schemes in several respects. First, some level of insurance fraud is almost inevitably incidental to pill mill schemes, as some drug customers use their Medicare, Medicaid, or other benefits to cover the cost of filling fraudulent prescriptions. Accordingly, even where a corrupt doctor runs a cash business and does not specifically seek to profit from fraudulent billings, signs of large scale fraudulent prescribing can often be detected by reviewing Medicare, Medicaid, or other insurance billings. For example, Dr. Washington Bryan was recently convicted in Los Angeles of structuring the cash proceeds of his fraudulent narcotic and AIDS medication business.[17] Dr. Bryan did not bill Medicare for seeing patients, but his patients used their Medicare benefits to fill the prescriptions that he issued. Thus, although Dr. Bryan ran a cash business, his prescriptions caused more payments by Medicare for Schedule II narcotics than any other doctor in California, by more than double the next highest prescriber.

Second, while Medicare and Medicaid beneficiary recruitment is less prevalent in narcotic diversion schemes, investigators continue to come across it. For example, in August 2017, CDCA prosecutors indicted the operators of multiple clinics throughout the district for issuing fraudulent prescriptions for more than 2 million pills of oxycodone and other controlled drugs. The modus operandi of the scheme included using elderly Medicare beneficiaries to fill prescriptions in exchange for cash kickbacks, and three recruiters were among the 13 indicted defendants.[18]

Third, investigators nationally continue to combat fraud and kickback schemes involving expensive opioid products. A particularly notable example is the recent growth of prosecutions involving the fentanyl spray Subsys, an expensive drug manufactured by Insys Therapeutics that is indicated only for treatment of breakthrough cancer pain. A federal indictment against the company, its lead

[17] United States v. Bryan, No. CR 16-320-RGK (C.D. Cal. 2016).
[18] United States v. Matosyan et al., No. CR 17-480-PSG (C.D. Cal. 2017) (Of the 13 charged defendants, 1 pleaded guilty and the remaining 12 pleaded not guilty and, as of this writing, are awaiting trial).

executives, and other conspirators is pending in Massachusetts, and the United States Attorney's Office in Los Angeles and Department of Justice's Civil Division recently intervened in multiple False Claims Act actions against the company. The cases allege, among other things, that the company fraudulently induced insurers to pay Subsys claims for patients who did not have cancer, and paid kickbacks to doctors in the form of "speaker fees" to induce higher prescribing. Criminal cases have since been pursued across the country against practitioners who received "speaker fees" for fraud or diversion connected to their Subsys prescribing.[19]

Finally, doctors, pharmacies, and other practitioners who engage in diversion are often multi-faceted offenders who seek to profit from both narcotic diversion for cash and also from other types of health care fraud. Investigators in Los Angeles and nationally often target corrupt doctors or pharmacists engaged in both narcotic diversion and also fraudulent billings for urinalysis, blood work, compound drug claims, and claims for other expensive non-controlled drugs such as HIV medications or antipsychotics, or addiction treatment.

The prosecution against Berry and Dalibor Kabov, two brothers who owned Global Compounding Pharmacy, offers an apt example of practitioners simultaneously running an all cash narcotics scheme and a health care fraud scheme involving unrelated claims. The Kabovs made $3 million in cash from their narcotic sales. In addition in 2015, they initiated a separate fraud scheme through which, over a period of less than ten months, they submitted $2.6 million in fraudulent claims to a labor union insurance program, all for non-controlled compounded creams in the names of identity theft victims. The owner of a Long Beach "medi-spa" clinic recently pled guilty to accepting nearly $400,000 in kickbacks from the Kabovs (falsely portrayed as marketing fees) in exchange for supplying the sham prescriptions to them.[20]

Similarly, the Kabovs conspired with a medical doctor, Joseph Altamirano, to perpetrate the narcotic diversion scheme. Altamirano took cash kickbacks from the Kabovs in exchange for writing narcotic prescriptions in the names of identity theft victims whom he never met or examined. Altamirano also recently pled guilty in Los Angeles for perpetrating an entirely unrelated scheme to profit from

---

[19] *See generally* Evan Hughes, *The Pain Hustlers*, N.Y. TIMES MAGAZINE, May 2, 2018.

[20] United States v. Carey, No. CR 17-256-DMG (C.D. Cal. 2017).

fraudulent claims to Medicare for durable medical equipment prescriptions.[21]

Often, combining a bird's eye view of controlled drug and insurance billing data for such practitioners easily reveals these "Jekyll and Hyde" type practices. Indeed, in August 2017 the Department of Justice announced the formation of the Opioid Fraud and Abuse Detection Unit, which engages in intensive data analysis to identify opioid-related fraud and diversion.[22]

Even for other investigations not directly stemming from that new initiative, it is important to cross-check information from narcotics databases and insurance databases (Medicare, Medicaid, etc.) for red flags, even those unrelated to controlled drugs. Some of the most successful narcotic diversion prosecutions in Los Angeles have involved partnerships between the DEA and other agencies such as HHS-OIG, the Department of Labor, or state agencies, initiated based on this type of intelligence sharing. Doing so may result in additional charges, restitution, or forfeiture of illicit proceeds. Additionally, a practitioner's participation in multiple criminal schemes can be compelling evidence of absence of mistake and can help paint an overall picture of a health care professional who made little effort to engage in legitimate treatment of patients.

IV. Health care fraud trends affecting private insurance programs

Health care fraud involving private health insurance programs continues to rise. This is a significant problem given the wide reach of private health insurance plans, which provide coverage for the majority of Americans—in 2016, 2/3 of Americans received health insurance coverage under a private health insurance plan.[23] Fraud involving private insurance plans increases health care costs for all Americans.

Numerous significant cases addressing fraud against private health insurance plans have been prosecuted in the CDCA. In February

---

[21] United States v. Altamirano, No. CR 15-321-GW (C.D. Cal. 2015).

[22] Press Release, U.S. Dep't of Justice, Attorney General Sessions Announces Opioid Fraud and Abuse Detection Unit (Aug. 2, 2017).

[23] *Health Insurance Coverage in the United States: 2016*, U.S. CENSUS BUREAU, https://www.census.gov/library/publications/2017/demo/p60-260.html.

2018, an indictment was unsealed that charged two defendants in a fraud scheme that involved more than $250 million in allegedly fraudulent claims submitted to private insurance companies.[24] The case arose out of a scheme involving multiple companies connected to the "1-800-GET-THIN" program, which marketed elective lap-band weight loss surgeries and advertised prominently on freeway billboards throughout southern California for many years. The indictment charged two individual defendants—one doctor and one former doctor—with devising a fraud scheme to induce private insurance plans to authorize payment for lap-band surgery, which they did not normally cover. The scheme operated by referring prospective lap-band recipients for otherwise unnecessary sleep studies, which were then falsified in order to establish a second reason (a "co-morbidity") such as sleep apnea, that could be presented to the patient's insurance company to fraudulently obtain authorization for payment for the lap-band procedure.

Photo 2: Defendant Mirando submitted millions of dollars' worth of fraudulent claims for services his holter devices did not perform, such as brain studies, oxygen tests, and 30-day recordings. The ads, which he designed, were introduced at trial to prove that Defendant Mirando never advertised the services and, in fact, advertised only the services the devices could perform.

[24] United States v. Julian Omidi, et al., No. CR No. 17-401-DMG (C.D. Cal. 2017) (The defendants pleaded not guilty and, as of this writing, are awaiting trial).

Other cases involving private insurance have been prosecuted with great success. In October 2017, the owner of a lab that submitted more than $8 million in claims to dozens of private insurance companies for heart monitoring tests and other procedures that were never performed, was sentenced to 97 months in prison.[25] (See Photo 2). In September 2017, a fugitive doctor who submitted more than $44 million in fraudulent claims to private insurance companies for unnecessary cosmetic procedures was sentenced in absentia to 20 years in prison.[26]

In addition to the health care providers, insiders at the insurance companies are also potential contributors to the fraudulent schemes and should be considered for prosecution in appropriate cases. For example, an indictment unsealed in May 2018 charges a former fraud investigator in the Special Investigations Unit (SIU) at Anthem Blue Cross with conspiracy to commit health care fraud based on his role in a $20 million private health insurance scheme.[27] The indictment alleges that, in exchange for cash payments, the former SIU investigator provided confidential information that he obtained from Anthem's internal systems to a co-conspirator, who owned medical clinics in southern California, so that the co-conspirator could better evade Anthem's fraud detection methods when submitting fraudulent claims.

"Sober living homes" have also given rise to a number of fraud prosecutions. The addiction treatment industry has grown dramatically since the passage of the Paul Wellstone and Pete Domenici Mental Health Parity and Addiction Equity Act of 2008, which requires insurers to pay for rehabilitation services. The Affordable Care Act of 2010 further expanded coverage. Private insurance covers this category of treatment for millions of working and middle class Americans. Annual spending by private insurers on opioid addiction alone rose more than 1,000% in the five year period ending in 2015, to roughly $721 million, according to Fair Health, an independent nonprofit that maintains a database of private insurance

[25] United States v. Michael Mirando, No. CR No. 16-215-PA (C.D. Cal. 2016).
[26] United States v. David M. Morrow, et al., CR No. 15-099-JLS (C.D. Cal. 2015).
[27] United States v. Roshanak Khadem, et al., No. CR No. 18-288-SVW (C.D. Cal. 2018) (The defendants pleaded not guilty and, as of this writing, are awaiting trial).

claims.[28] In southern California, Florida, and other sunny climates, fraudulent operators lure individuals with drug addiction issues—a group that has grown as the opioid epidemic has spread—from around the country to stay at the sober living homes they purport to run, promising programs that will assist the individuals to "get clean." Unfortunately, in too many cases, the people in charge of the sober living homes do not provide treatment for the addiction issues but, instead, use their clients' insurance information to submit fraudulent claims to insurance companies. As a further harm, when their insurance benefits are exhausted, the clients are often put out on the street with no resources or assistance. The impact of these practices on the homelessness problem has become so significant that the California State Senate is considering legislation that would specifically address the practice of "patient brokering"—that is, recruiting individuals in need of substance abuse treatment in exchange for kickbacks.[29]

The significance of substance abuse treatment fraud and the importance of prosecutions addressing fraudulent practices in sober living homes is reflected in the 27-year sentence obtained in May 2017 by the United States Attorney's Office in Miami for the owner of a sober living home who pleaded guilty to health care fraud, money laundering, and sex trafficking charges based on his operation of a sober living facility in south Florida.[30] In light of the ongoing opioid epidemic, the possibility of fraud and abuse in the operation of sober living homes should continue to command the attention of prosecutors.

Private insurance plans, including plans operating under state workers' compensation regimes, have also become the victims of sophisticated kickback and bribe schemes, ranging from the referral of surgery patients to collusive hospitals, to the steering of prescriptions for expensive compounded drugs[31] to collusive pharmacies. In the

---

[28] FAIR HEALTH, INC., *The Impact of the Opioid Crisis on the Healthcare System: A Study of Privately Billed Services*, at 3 (Sept. 2016).

[29] S. 1228, 2017–2018 Leg., Reg. Sess. (Cal. 2018).

[30] United States v. Kenneth Chatman et al., No. CR No. 17-80013-DMM (S.D. Fla. 2017).

[31] In general, "compounding" is a practice by which a licensed pharmacist, a licensed physician, or, in the case of an outsourcing facility, a person under the supervision of a licensed pharmacist, combines, mixes or alters ingredients of a drug or multiple drugs to create a drug tailored to the needs of an individual patient.

past, typical kickback and bribe schemes involved hidden cash payments made to referral sources, usually "cappers" or "marketers," but also sometimes including doctors and other medical professionals. In contrast, recent kickback and bribe schemes affecting private insurance victims have relied on a variety of "bogus" or "sham" business arrangements to hide referral payments in plain sight.

The investigation of Pacific Hospital of Long Beach (hereinafter Pacific Hospital), designated as "Operational Spinal Cap," highlights the widespread use of various "sham" business arrangements to disguise referral payments. In early 2014, the ex-CEO of Pacific Hospital pleaded guilty to charges stemming from the payment of illegal kickbacks and bribes to facilitate the referral of patients to the hospital. The kickback scheme, which spanned a 15 year period and generated a cumulative total of more than $950 million in kickback tainted claims to federal, state, and private insurers, has been identified as "California's largest case of medical fraud."[32] Other recent health care cases across the country, including compounding pharmacy fraud investigations, have similarly involved massive referral-for-kickback schemes—ostensibly relying on contractual arrangements that were, in fact, devoid of any purpose other than to confer a patina of legitimacy to the scheme—that quickly generated thousands of referrals and corresponding kickback-tainted insurance claims that were submitted to federal, state, and private insurance programs.

The sham business arrangements used in these referral schemes have varied widely based on the creativity of the co-schemers.[33] These business arrangements, often memorialized in written contracts (See Photo 3), do not reflect the parties' true intent or understanding. For example, the contracts do not specify that one purpose for the arrangement or payment under the contract is to influence referrals. Several of the agreements at issue in Operation Spinal Cap explicitly disclaimed that payments under the contracts were for referrals. The sham nature of the contracts can be inferred from the fact that they provided compensation (1) for services that were already being provided to the hospital by other paid parties; (2) for services, for

[32] *See* Steven Mikulah, *Kickbacks, Bribes, and the Horrifying Truth Behind California's Largest Medical Fraud Scandal*, L.A. MAGAZINE, March 21, 2016.
[33] *Cf.* Weiss v. United States, 122 F.2d 675, 681 (5th Cir. 1941) ("The law does not define fraud; it needs no definition; it is as old as falsehood and as versable as human ingenuity.").

example, "research and development" that were not, in fact, provided; or (3) in amounts that were far in excess of the value of the goods or services being provided.

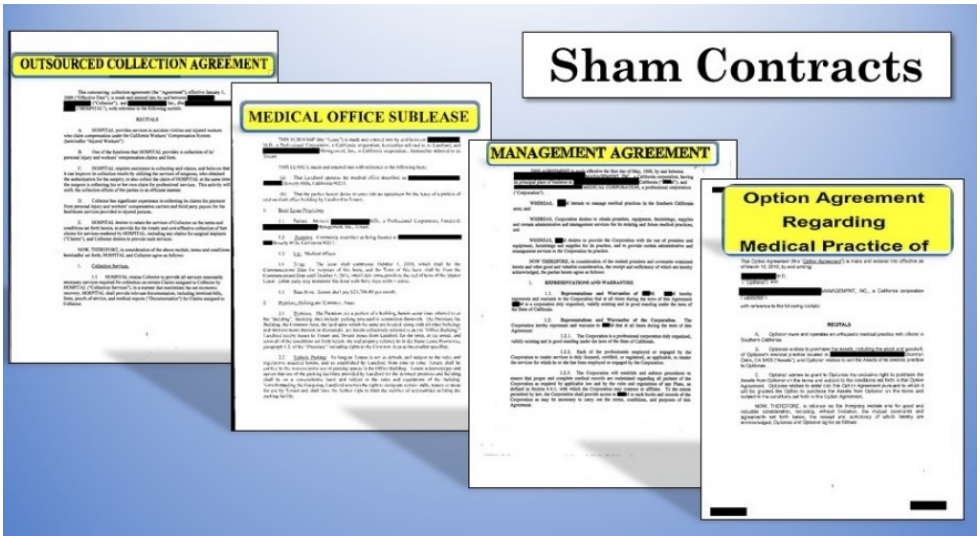

Photo 3: Examples of Business Contracts Used to Conceal Illegal Kickbacks

The written contracts at issue in Operational Spinal Cap included:[34]

Option agreements

Physicians were paid for an "option" or "right to purchase" their medical practices, but the option was never intended to be exercised. Red flags associated with these option agreements included the lack of any real practice valuations, multi-year durations for the option payments (as opposed to a short term option period to support actual negotiations regarding the purchase of the practice), the active referral relationship between the physician and the hospital, and the fact that the hospital never once exercised an option to buy a medical practice.

Management agreements

Under a typical management services agreement, a management company will order and purchase the medical and office supplies required for the operation of a practice, and manage information

[34] *See* Plea Agreement at 13, United States v. Drobot, No. 8:14-cr-00034-JLS (C.D. Cal. 2014), ECF No. 7.

systems services, bookkeeping, accounting services, billing and collection services, and marketing. In exchange, a managed physician compensates the management company for providing these services. A legitimate management fee typically covers the costs associated with managing the medical practice and provides a profit for the management company.

Pacific Hospital used a closely affiliated management company to induce managed physicians—through heavily discounted management fees—to send patient and ancillary service referrals to the hospital and affiliated entities.[35] The discounts on the management fees caused the management company to operate at a loss, but this was not a concern because the discounts incentivized managed physicians to generate business for the closely affiliated hospital. The hospital subsidized the affiliated management company, thus enabling the scheme to continue.

The use of an outwardly independent management company to support what is, in fact, an affiliated hospital is not uncommon. Prosecutors should carefully review management agreements to ensure that they are not being used to disguise unlawful kickback arrangements designed to generate patient referrals.

Sublease and rental agreements

Subleases and rental agreements are a common device used to disguise kickbacks.[36] In the context of Operation Spinal Cap, the hospital or its affiliated management company entered into a sublease or rental agreement with a referral source, and agreed to make payments in excess of the fair market value of the space being leased based on an unwritten understanding that the referral source would refer patients to the hospital. In extreme cases, the subleased spaced is never even used.[37] In other cases, the payments far exceed the fair

[35] *See* Plea Agreement at 34–36, United States v. Capen, No. 8:18-cr-00124-JLS (C.D. Cal. 2018), ECF No. 6.

[36] *See Special Fraud Alert: Rental of Space in Physician Offices by Persons or Entities to Which Physicians Refer*, OFFICE OF THE INSPECTOR GEN., https://oig.hhs.gov/fraud/docs/alertsandbulletins/office%20space.htm.

[37] *See, e.g.,* McNutt *ex rel.* United States v. Haleyville Med. Supplies, Inc., 423 F.3d 1256, 1258 (11th Cir. 2005) (noting that to conceal the nature of the kickback payments, a co-conspirator characterized each check as "rent" in the "memo" portion of the check).

market value of the lease when the size of the space actually used, and the frequency of the use, is taken into consideration.

Services agreements

In Operation Spinal Cap, kickbacks to referring physicians were also disguised as payments for purported consulting, research, directorship, and billing and collection work that was either never performed or whose actual value fell far below the amount of the payments. Nor did the hospital have an appropriate business justification to enter into such agreements.[38]

Significantly, these business arrangements are not unique to hospital referral schemes. Variations of these arrangements featured prominently in recent compounding pharmacy fraud and kickback investigations. For example, compounding pharmacies recently generated massive prescription volumes using allegedly "bogus" services agreements, including employment and consulting agreements, to funnel referral payments from the pharmacies to referral sources. Purported employment agreements would falsely designate "marketers," who functioned exclusively as independent contractors, as "employees" in a misguided attempt to fall under a kickback "safe harbor." In reality, the pharmacies did not control these "marketers," who often worked for other pharmacies, set their own schedule, and were compensated almost exclusively for referrals. Similarly, "consulting agreements" for a laundry list of largely unnecessary, redundant, or irrelevant services have been used to justify the payment of substantial kickbacks for referrals.[39] Ironically, these written agreements had the unintended effect of helping law enforcement establish the knowledge and intent of co-schemers who committed specific intent health care offenses.

Prosecutors have a broad array of charging options in private health insurance cases, including mail fraud, wire fraud, health care fraud, false statements relating to health care matters, money laundering, and obstruction statutes. One limitation in prosecuting cases

---

[38] *See also* United States v. Anderson, 85 F. Supp. 2d 1047, 1057 (D. Kan. 1999) (finding that "services contract" used to facilitate payments by hospitals to physicians for ostensible services when they performed little or no services violates the law).

[39] *See* United States v. LaHue, 261 F.3d 993, 999 (10th Cir. 2001) (finding "consulting agreement" used to camouflage underlying agreement to give remuneration for patient referrals illegal).

involving private health insurance schemes is that the federal anti-kickback statute only applies to services for which payment is to be made under a "Federal health care program."[40] Despite this limitation, criminal charges for kickbacks in the private insurance context can be pursued using an honest services mail/wire fraud charge and/or charges under the Travel Act.[41] Courts have recognized that kickbacks to doctors can involve the kind of breach of a fiduciary duty that the Supreme Court in *Skilling v. United States*[42] required in order to support an honest services prosecution.[43] Under the Travel Act theory, California and other states have multiple statutes that outlaw payment of bribes for services that are to be covered by a broad range of health insurance companies, and these violations of state law provide the basis for prosecuting the underlying unlawful kickback-for-referrals schemes.[44] These charging theories give prosecutors the tools to pursue criminal actors for the payment and/or receipt of kickbacks in the private insurance context, even though the federal Anti-Kickback Statute may not be an available option.[45]

V. Conclusion

Given the size and complexity of the health care industry, it is not surprising that the schemes used to bill government and private

---

[40] 42 U.S.C. § 1320a-7b(b).

[41] *See* 18 U.S.C. §§ 1341, 1343, and 1346 (honest services); 18 U.S.C. § 1952(a)(3) (Travel Act).

[42] Skilling v. United States, 561 U.S. 358 (2010).

[43] *See, e.g.*, United States v. Nayak, 769 F.3d 978, 981–84 (7th Cir. 2014); United States v. Neufeld, 908 F. Supp. 491, 500 (S.D. Ohio 1995).

[44] *See, e.g.,* CAL. BUS. & PROF. CODE § 650 (prohibiting bribes and kickbacks to licensed medical professionals); CAL. INS. CODE § 750(a) (prohibiting bribes and kickback to providers who submit insurance claims); CAL. LAB. CODE § 3215 (prohibiting kickbacks in connection with the California Workers' Compensation System); *see also* N.Y. PENAL. LAW § 180.05 (outlining New York commercial bribery in the second degree which prohibits, *inter alia*, a fiduciary from accepting any benefit, not disclosed to the principal, to influence the fiduciary's conduct in relation to the principal's affairs); N.J. STAT. ANN. § 2C:21-10 (outlining New Jersey commercial bribery cause of action prohibiting, *inter alia,* physicians from accepting any payment in breach of a duty of "fidelity").

[45] *See* Robert M. Wolin*, Kickbacks and Commercial Bribery: Another Touchstone to Consider*, BAKERHOSTETLER (Apr. 1, 2016), https://www.healthlawupdate.com/2016/04/kickbacks-and-commercial-bribery-another-touchstone-to-consider/.

insurers and to exploit the current opioid epidemic are constantly evolving to maximize illicit profits and evade detection. As prosecutors, we must also continue to evolve to address these schemes. By using data analytics tools to identify significant health care fraud perpetrators and developing innovative charging theories to ensure that fraud in all aspects of the industry is addressed, we can take important steps in this evolution.

About the Authors

Ranee A. Katzenstein has been an Assistant United States Attorney in the Central District of California since 1997, where she serves as the Chief of the Major Frauds Section. Among other supervisory positions, Ms. Katzenstein served as the district's Chief Assistant for Trials, Integrity and Professionalism in 2016–2017. Ms. Katzenstein earned her law degree from Stanford University.

Diidri Robinson recently moved to the private sector. Prior to the move, Diidri Robinson was an Assistant Chief with the United States Department of Justice's Criminal Division, Fraud Section, where she supervised the Medicare Fraud Strike Force prosecutors in Los Angeles, New Orleans, and Baton Rouge. Robinson served as the coordinator for the 2018 National Health Care Fraud and Opioid Takedown, in which 601 defendants were charged with more than $2 billion in fraudulent billings. Robinson joined the Fraud Section from the United States Attorney's Office in Jacksonville, Florida, where she prosecuted a wide range of criminal offenses, including white-collar fraud, narcotics and firearms trafficking, violent crimes, and child exploitation. She also previously served as a commercial litigation associate at Holland & Knight. Robinson began her legal career as an Assistant State Attorney in Jacksonville, where she was recognized as the Outstanding New Felony Prosecutor.

Benjamin Barron has been an Assistant United States Attorney in the Central District of California since 2008, where he serves as Deputy Chief of the district's OCDETF Section. Since 2011, Mr. Barron has coordinated the section's opioid and prescription drug diversion program, including overseeing criminal prosecutions, community outreach efforts, and law enforcement training. Mr. Barron received an EOUSA Director's Award and an OCDETF Director's Award in recognition for this work.

Ashwin Janakiram is an Assistant United States Attorney for the Central District of California, in the Major Frauds Section, and

currently serves as the office's Home Health Agency Coordinator. Since joining the United States Attorney's Office in 2012, Ashwin has prosecuted a wide variety of health care related cases, among others, including investigations concerning hospitals, compounding pharmacies, surgical hardware distributors, home health agencies, and physicians. These investigations included allegations of kickbacks, money laundering, and health care fraud. Before joining the United States Attorney's Office, Mr. Janakiram was an associate at Sidley Austin LLP in Chicago. He holds degrees from Miami University of Ohio and the University of Kansas School of Law.

Alexander F. Porter is an Assistant United States Attorney for the Central District of California in the Major Frauds Section. He currently serves as the office's Criminal Health Care Fraud Coordinator. From 2013–2016, Mr. Porter served as a Trial Attorney in the Fraud Section of the Criminal Division, where he prosecuted criminal health care fraud cases as part of the Medicare Fraud Strike Force in Los Angeles. Mr. Porter earned his law degree from the University of Southern California and his undergraduate degree from the University of San Francisco.

Pioneering a Modern Discovery Process: District of Alaska's Discovery Center

Bryan Schroder
United States Attorney
District of Alaska

Aunnie Steward
Assistant United States Attorney
District of Alaska

I. Introduction

The time is now for standardization of discovery processes. The explosion of electronic data has radically changed the nature of discovery in both criminal and civil cases in a relatively short amount of time. The volume of data gathered by parties has increased exponentially, and the tools necessary to process this data require more technical expertise. United States Attorney's Offices can no longer content themselves with ad hoc discovery practices developed at the advent of the copier and fax machine. A change is required.

All of our offices, no matter the size, will benefit from having a more standardized, defensible discovery system in place. When our office transitioned to a standardized discovery system over a year ago, there were pioneers in other districts that assisted us on the path, as well as some tools made available by the Department. Over the past two years, the authors were able to work together with our colleagues to identify problems, find solutions, and transition to a standardized system within our office. With the resources now available from the Department, the time required for other districts to transition should be significantly shortened. This short organizational study explains how we tackled the problems caused by the increased volume and complexity of electronic data in discovery and made significant internal organizational and workflow changes to adapt to the modern discovery world.

II. The data tsunami

The past ten years has seen an almost epidemic growth of electronic devices that generate digital evidence in criminal cases. In 2009, discovery in the average case in the District of Alaska consisted of 95 pages of documents and 2 audio files. By 2017, that average had grown to 302 pages of documents, 92 audio files, and 6 video files. This is consistent across the United States Attorney's Office community, which saw as much as a 300% increase in electronic evidence in some districts from 2011–2014.

Why such rapid growth? The arrival of the smart phone was the primary driver. The iPhone was released in 2007. In 2011, only 35% of U.S. residents owned a smartphone. By 2018, that number increased to 77%.[1] In the 18 to 29-year-old age group, the level increases to 94%.[2] Tablets were owned by less than 10% of the population in 2011, but are now owned by 50%.[3] Home computer ownership has remained constant, at about 75% since 2008.[4]

Electronic evidence has added considerably more volume to our case discovery. An average iPhone download produces three to seven gigabytes (GB) of data, equivalent to 5,000 to 9,000 pages of paper. IPads hold even more, with an average download containing seven to nine GB of data, equivalent to 9,000 to 12,000 pages of paper. A home or laptop computer, especially with removable storage in the form of CDs, USB flash drives, or hard drives, can yield much greater amounts of data.

The rapid growth of social media has also fueled the data explosion. In 2018, 69% of the U.S. population has a social media account, up from less than 10% in 2005.[5] That number is 88% for the 18–19 year-old age group.[6]

Texting also has become more significant as a source of evidence. Facebook Messenger has more than 1.3 billion users and is adding 100 million new users every five to six months.[7] Those users have

---

[1] PEW RESEARCH CTR., MOBILE FACT SHEET (Feb. 5, 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] PEW RESEARCH CTR., SOCIAL MEDIA FACT SHEET (Feb. 5, 2018).
[6] *Id.*
[7] Ben Parr, *Why You Need to Add Facebook Messenger to Your List of Marketing Tools*, INC. MAGAZINE, Dec. 21, 2017.

7 billion conversations a day.[8] WhatsApp, which is especially popular outside of the United States, has 1.5 billion users.[9]

Finally, video evidence is becoming ubiquitous. The use of video surveillance cameras continues to rapidly expand and is a consistent source of evidence in a variety of cases. Video evidence is also generated by individuals and stored on smart phones or on social media sites. Law enforcement agencies generate their own video in the form of interviews, undercover recordings, dashboard cameras, and more recently, body cameras on individual officers.

In addition to there being a vastly greater amount of data available, the data is also much more complicated to process than were hard copy documents. First, electronic data comes in a variety of formats. Text documents, databases, and especially audio, photo, and video files come in a wide variety of formats, and sometimes in formats proprietary to the systems that recorded the data. Second, methods of securing data make it difficult to process as discovery. Data is now often encrypted, as well as protected by passwords, certificates, or digital signatures. As the data is pulled into a United States Attorney's Office's server or cloud system, all of those protection systems have to be managed. Finally, the terms of the "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" promulgated by the Department of Justice and Administrative Office of the U.S. Courts (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG) in 2012 generally call for the party producing electronic discovery to provide the metadata when available and to make text documents OCR searchable. This also adds complexity to the processing and production.

III. Outdated processes

During the early days of the Data Tsunami, it was common practice for agents to burn a disc of "everything" and leave it on the chair of an Assistant United States Attorney or paralegal with an agency case number scribbled on the disc that only made sense to the agent. The disc could contain one document or the equivalent of a room full of

---

[8] *Id.*

[9] *Number of monthly active WhatsApp users worldwide from April 2013 to December 2017 (in millions)*, STATISTA, https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ (last visited October 18, 2018).

documents, but the recipient had no way of knowing what was supposed to be on the disc versus what it actually contained. Here is an example of how this played out in a case from our district.

Agents in a complex fraud case had diligently scanned in many boxes of documents seized pursuant to multiple search warrants. An administrative staff member within the law enforcement agency was asked to burn the documents to a disc and provide it to the United States Attorney's Office. Unfortunately, the staff person inadvertently burned the wrong file to the disc, so it contained only one unrelated item. It was not until the eve of trial that trial attorneys discovered that the actual search warrant documents had never been produced. The paralegal who received the disc at the United States Attorney's Office had no idea what was supposed to be on the disc and dutifully processed and produced that one item. We were unable to explain to the court why the search warrant materials had not been produced, because there was no system in place for tracking the information provided by the agency to the United States Attorney's Office.

This incident highlighted the need for a way to track information produced from the agency to the United States Attorney's Office. Some tracking was being done at the United States Attorney's Office as discovery was produced to defense counsel, but nothing was being done to track the receipt of materials from the agency. It also highlighted the need to understand how each agency managed its data related to the case; that is, what internal tracking system did it have, what system of organization did it use, and how did it ensure "everything" was produced to the United States Attorney's Office?

Another issue crippling the office was the substantial time spent by paralegals manually copying reports in Adobe Acrobat from agencies because security certificates did not allow bates numbers to be put on the documents. The burden of redaction was also heavy on the paralegals, as it required late nights and weekends by all support staff. Compounding the problem was each individual Assistant United States Attorney's particular way of processing discovery. There was no standardization of bates numbering, redactions, or use of logs. Finally, there was the issue of the different types of data described above and the challenges of processing it for discovery. Each paralegal found his or her own way to manage the data, oftentimes relying on the IT staff. There was no standard way to process the high volume and different kinds of proprietary software (including audio and video surveillance from banks, local law enforcement, and other sources)

and cell phone extractions, and no set way to track the data as received and produced. It was an unsustainable effort on all fronts.

In 2014, the two of us were recruited to dig into some of these issues and try to fashion a solution. We started by making the rounds with our partner law enforcement agencies to better understand their practices. We also met with our support staff to get their input on the issues they identified. As the ones in the trenches grappling with the issues outlined above, they had the best insights into the problems. We also made contact with other districts that were working toward addressing similar issues.

The items identified in these discussions fell into the following categories: (1) finding efficiencies through standardization of processes and better use of technology; (2) better communication between agencies and the United States Attorney's Office, between Assistant United States Attorneys and support staff, and between the United States Attorney's Office and the defense bar; and (3) better tracking of materials from the agency all the way through to defense counsel.[10]

---

[10] Additional and more specific ideas included:

Finding efficiencies:

(1) Standardize what is to be redacted and who is doing the redacting, and encourage protective orders in lieu of redacting as much as possible.
(2) Standardize bates numbering for all Assistant United States Attorneys.
(3) Utilize the new high-powered Law PC computers to process discovery materials that could copy agency reports despite security certificates.

Better communication:

(1) Meet with all agencies and develop a point of contact at each one for purposes of discussing discovery issues as they arise.
(2) Meet with the Federal Defenders, the CJA panel attorneys, and the court to describe our efforts. Work to achieve buy-in.
(3) Hold regular meetings with support staff to address discovery issues as they arise.

Better Tracking:

(1) Institute a tracking receipt that every agent has to fill out when dropping off discovery, describing what is on the disc and providing the case name.
(2) Where possible, utilize agency indexes to check and make sure we are receiving everything that we need.
(3) Generate better logs for materials produced to defendants.
(4) Utilize the new database Eclipse for discovery review, and require all Assistant United States Attorneys to tag each piece of discovery to be produced or not produced.

IV. Tools

During the Data Tsunami, the Department had tried to keep pace by providing powerful tools to handle digital evidence. Law PC computers and software allowed for processing large amounts of data faster than was possible with normal computers and also offered the ability to process password and security protected data more easily.[11] The Department had also rolled out the Eclipse database as a replacement for Ipro as a review and viewing tool.

These were great tools, but they were not effectively utilized by our office and—from what we understand—that is true of a number of offices. In our office, that was because those tools required a combination of IT knowledge and familiarity with Automated Legal Support (ALS) and discovery processes we had not assembled into one team. We had attempted to integrate Law PC into our existing discovery process and provided training to our paralegals. We discovered that Law PC was too complicated for part-time use. The system could lead to significant gains in efficiency but only when the operators gained the level of expertise only available with regular, day-to-day use. These tools turned out to be the keys to the kingdom. We just did not recognize their power or have the ability to make them work for us at the time. But there was at least one district that had figured out how to use these tools successfully, and that was our neighbor to the south in Oregon.

V. United States Attorney's Office collaboration

During the investigative phase, we were alerted by a colleague that the District of Oregon had recently made a presentation on the same issues we were tackling. This tip led us to contact Assistant United States Attorney Geoffrey Barrow and discovery guru Susan Cooke in Portland. Their district had been through its own discovery snafu and had spent a year doing the heavy lifting of identifying discovery challenges and finding solutions. They were much farther down the path toward solutions than was our district, so we started contacting them regularly for information and advice. Ultimately, we were invited to travel to Oregon, along with our colleagues from the Eastern District of California, to view the system they had set up.

[11] EOUSA has now provided an even more robust processing tool, NUIX.

The success of the District of Oregon's system was built on centralization of processing. They created a "Discovery Center" where all of the ALS staff worked together using the high-powered computers that had been provided by the department (Law PC) to process discovery in a standardized way. The Oregon team is led by Susan Cooke, who had both ALS and IT familiarity. Projects could be left to run overnight instead of manually duplicating every page in Adobe Acrobat by a paralegal working nights and weekends. As Susan Cooke described it, this was their answer to the information revolution. Much like the industrial revolution, they were creating an efficient assembly line of processing data. Oregon had spent significant money on bringing in Law PC trainers from the private sector to train their staff. Following our meeting, the District of Oregon was very generous in allowing Susan Cooke to travel to Alaska and provide training to our district. Susan conducted four days of training that included segments for managers and Assistant United States Attorneys, but its primary purpose was for support staff to learn to use the new technology effectively.

We also received advice and helpful materials from other districts, including Colorado and North Carolina-Western. In particular, John Haried from the Colorado United States Attorney's Office had generated several checklists and letters to help track discovery and inform agencies of our discovery obligations. Not coincidentally, John Haried and Susan Cooke, two of our expert advisors used in creating our process, subsequently became part of an eLitigation Advising Team at Executive Office for United States Attorneys (EOUSA) to help all United States Attorneys' Offices tackle eLitigation issues. The Advising Team has set up a peer to peer advising and training program similar to what we did informally with Oregon. Selected Assistant United States Attorneys and litigation technologists from United States Attorneys' Offices and the Office of Legal Education (OLE) work intensively with individual districts on eLitigation issues. The United States Attorneys' Offices wanting more information about the Advising Team should contact Tammy Reno, Acting Counsel for Legal and Victim Programs, at EOUSA.

VI. Forming the discovery center

In the summer of 2016, after studying the problem, identifying the available tools, and consulting with our local law enforcement partners and United States Attorney's Office colleagues, it was time to make some decisions. The United States Attorney in Alaska at the

time, Karen Loeffler, along with the rest of the management team, were supportive. The authors proposed the formation of a Discovery Center, similar to what the District of Oregon had in place, but smaller in scale.

We decided to create a separate physical space in the office for the Discovery Center. Part of that decision was symbolic. We were making such a significant change in how we did business that we wanted to make clear it was a structural change, both physically and in our business processes. We had a litigation support room, so all the Law PC computers were installed in that space.

The most important decision was the composition of the Discovery Center staff. Initially, we decided to dedicate two full time staff members to the center. At the time, our office had one assigned ALS position but, as a practical matter, that person had been incorporated into the IT Department. Since our paralegals had become discovery specialists and were familiar with the legal requirements, we started with one of our most experienced paralegals. However, it was clear that additional technical expertise was also required.

The newest member of our IT department had been assigned to a recent high profile case with extensive discovery, and she had been essential in making sure the trial team had no significant discovery issues. She also never shied away from a challenge. It was a natural fit. Additionally, both Discovery Center staffers were good communicators, creative problem solvers, and were confident in their abilities. Those traits were necessary because we wanted the Discovery Center to reach out to the law enforcement agencies to form partnerships and be able to adapt and change processes as issues arose.

VII. Growing pains and changes

With the Discovery Center in place and the new tools of Law PC and Eclipse ready to be used, there was still a question of workflow. Previously, each Assistant United States Attorney had their own practice as to the timing of receipt of materials from agencies, when (or in some instances if) they reviewed the discovery, when and who redacted the materials, and how the materials were produced to defense counsel. We held several discussions with support staff, Assistant United States Attorneys, and the newly formed Discovery Center team, Kim Hooper and Jennifer Lotz, to arrive at a standardized workflow.

Kim Hooper created the following graphic to make it easy for everyone to understand our new work flow:

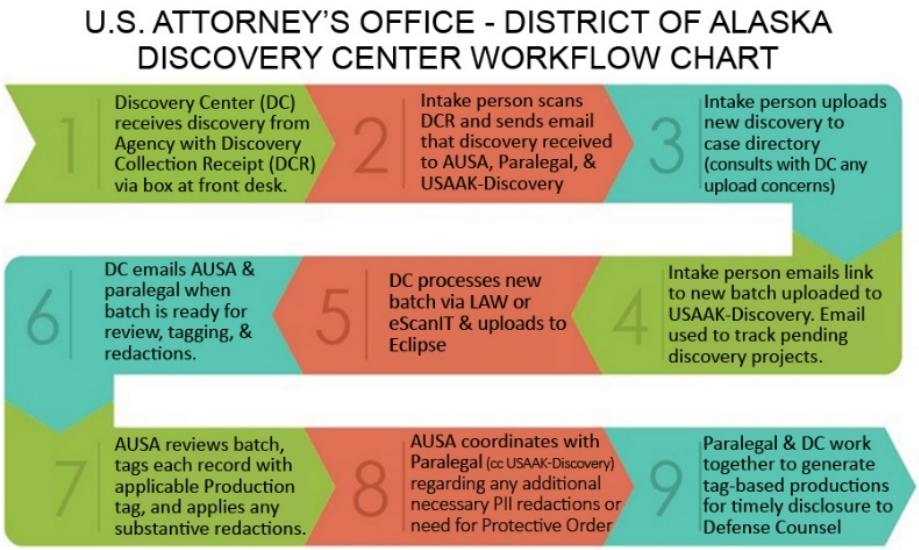

Figure 1. Discovery Center Workflow
Credit to Kim Hooper, United States Attorney's Office Discovery Center Alaska

Once the Discovery Center was set up, it was never intended to be a static operation. No project involving this level of personnel and process changes will achieve success without making adjustments and addressing problems as they arise. Moreover, because we were developing the Discovery Center almost from scratch, some of the decisions we made at the outset would require course corrections. As new challenges arose, it was important to maintain communication between agencies, Assistant United States Attorneys, support staff, and the defense bar, and to adapt and revise processes as necessary. In addition to workflow, some of the challenges navigated in the early stages of implementing the Discovery Center by Jennifer and Kim included gauging the volume of data to be processed month to month, figuring out averages, and planning and resourcing accordingly. This has been incredibly helpful for decision making by management on how to dedicate resources.

Ultimately, this information on volume, along with other needs of the Center, supported the conclusion that a third staff position needed to be added to the Discovery Center. That proved to be the case because of the importance of the intake process. One of our goals was

positive control of the data from initial receipt to the production to the defendant. Intake proved to be much more of an issue than we suspected. Previously, agents provided evidence directly to the Assistant United States Attorney, legal assistant, or paralegal. We decided that intake needed to happen directly with the Discovery Center. That proved to be too time consuming for the two original staff members. Our first attempt at a fix was to rotate a legal assistant to be the weekly intake staffer. That worked reasonably well, but the legal assistants were extremely busy with their normal duties. We tried shifting the intake responsibility to one of our front desk staff, who did the work diligently, but had limited knowledge of the parts of the process that were to follow, especially the technical aspects. The third change turned out to be the charm. We converted a legal assistant contract position into the Discovery Center and hired a contractor with sufficient technical skills to make the intake process efficient.

Another part of our goal of maintaining control of the data was to document the process from beginning to end. This started with intake. We developed an intake receipt for the case agent to fill out when dropping off the data. The receipt identifies the case name, case number, type of media provided, name of the agent, and general contents of the material. The end result of the discovery Center workflow was to provide defense counsel with a "discovery manifest" at the time of production. The manifest allows defense counsel to identify the electronic files that are produced. The document started as a simple listing of the files names, but our local CJA panel of defense attorneys asked that we add a basic description of the file, that is, "302 of interview with John Smith." We decided that was a fair request, and the agencies are now providing a description that is included by the Discovery Center in the manifest that is produced.

To document how we get from the intake receipt to the discovery manifest, we instituted a work order system. The intake person in the Discovery Center creates a work order for processing whenever new material is dropped off. Also, any staff members who want other types of litigation support, such as video or audio file conversions, trial exhibits, etc., must initiate a work order. The work order database and system were developed by the District of Minnesota. Eventually, anyone on the staff will be able to sign on and see the status of their work orders.

Finally, at the time we instituted the Discovery Center, the production of discovery to defense attorneys was done by the Center

staff. However, our goal was to eventually reintegrate the paralegals into the discovery process to do production. Recently, we have been able to provide sufficient training to the paralegals on Eclipse that they have taken over production duties to the defense.

This raises an important issue: training. One of the most key aspects of our process change was to have a consistent method of reviewing files to make discovery decisions. We decided to use Eclipse as our review tool. While Eclipse is powerful, it requires training for all Assistant United States Attorneys, and was daunting to some of the staff. Group training was provided to give a general overview of Eclipse to Assistant United States Attorneys, but the bulk of the training was conducted by Discovery Center staff one-on-one. They worked with Assistant United States Attorneys at their desks and walked them through their own case projects. Our Discovery Center staff estimates that 60–70% of the Assistant United States Attorneys took to the change quickly. Some Assistant United States Attorneys complained when cases had individual processing problems, but the management team, especially the Criminal Chief and Deputy Criminal Chief, were resolute that all Assistant United States Attorneys adopt the new process. Management support was critical to the success of the Center.

In the end, most if not all Assistant United States Attorneys accepted the change because they knew a more formal system helped to protect them against accusations of discovery violations. Also, once the learning curve was surmounted, the interface with Eclipse was a much easier tool to navigate for discovery review than had previously been available.

VIII. Current status

The District of Alaska Discovery Center project is unquestionably a success. The Assistant United States Attorneys are now accustomed to using Eclipse to review discovery. Moreover, we now have a record of that review, assuring the management of the Criminal Division that all discovery has been reviewed by the Assistant United States Attorney and decisions to produce or withhold are documented. The Discovery Center staff have developed an expertise gained by seeing all the types of discovery material and discovery issues that come up in the office. This expertise provides for efficiencies and better quality control.

Most agents are happy with the new system as well. They appreciate having a one-stop shop to bring all of their materials that

is not case or Assistant United States Attorney specific. It is easier for them to have a single, consistent process to follow and to know whom to contact regarding discovery issues. They also appreciate the timeliness of the system and tracking capability. We have mostly achieved our goal of accurately tracking discovery from intake to distribution. Defense counsel also like the common organization, discovery manifests, and that files include metadata and are OCR searchable. Defense counsel and their support staff appreciate having a contact for technical issues that arise in the materials they receive.

We also invited the district judges and magistrate judges to tour the Discovery Center and be briefed on our new process. They now understand the efforts we have made to implement an efficient and effective discovery system. They understand that the system benefits all parties. Our tour paid quick dividends. The magistrate judges in Alaska regularly required production of discovery within seven days of arraignment. We had been requesting a two week deadline for some time but to no avail. After touring the Discovery Center and understanding our commitment to responsibly meeting our discovery requirements, they quickly agreed to extend the deadlines.

We have successfully implemented the new discovery process in our main office in Anchorage and are moving to implement it in our branch offices in Juneau and Fairbanks. The Discovery Center staff has also been working with our Civil Division to gain efficiencies in civil discovery. Our Civil Division does extensive medical malpractice defense, and we have found our Discovery Center tools useful in organizing medical records. Recently a proposed project for a case being handled by the Civil Division was going to cost an estimated $10,000 for processing of discovery materials related to medical records. The Discovery Center was able to step in and do the entire project in a much more efficient manner for no additional cost.

Most importantly, we have realized the efficiencies that we needed to survive in the modern eDiscovery world. Prior to establishing the Discovery Center, our Criminal Division paralegals worked nights and weekends to keep up with discovery demands. In the months after the implementation of the Discovery Center, one paralegal went on extended military duty and another was out for a number of weeks with a medical issue. In previous years, that would have been a recipe for a discovery disaster. With the Discovery Center in place, we were able to keep up with the demand.

We are proud to have been part of the early-wave adopters of a standardized eDiscovery process and we are glad to help other

districts informally with advice and information, and also formally with our Discovery Center staff serving as mentors for EOUSA's peer-to-peer training program.

About the Authors

Bryan Schroder currently serves as the United States Attorney for the District of Alaska. He was appointed on November 9, 2017. He is a 1981 graduate of the U.S. Coast Guard Academy and a 1991 graduate of the University of Washington School of Law. Mr. Schroder is also one of the 15 United States Attorneys selected by Attorney General Sessions as a member of the Attorney General's Advisory Committee (AGAC). The AGAC represents the United States Attorney community, and provides advice and counsel to the Attorney General on matters of policy, procedure, and management impacting the Offices of the United States Attorneys.

Prior to becoming United States Attorney, Mr. Schroder served as the Acting United States Attorney for the District of Alaska, and previously served as the First Assistant United States Attorney and Chief of the Criminal Division. He also served in the Criminal division as an anti-terrorism prosecutor, and was the District Ethics Advisor. Prior to joining the Department, Mr. Schroder served 24 years in the U.S. Coast Guard and is a retired Captain.

Aunnie Steward is an Assistant United States Attorney in the District of Alaska. She also serves as Discovery Counsel for the District. She has been with the Department since 2003, including three years in the Environmental Crimes Section (ECS) as a Trial Attorney and now twelve years in the District of Alaska. She received the Department of Justice John Marshall Award as part of a multi-jurisdictional prosecution team while with ECS. She has served as a facilitator for the Office of Legal Education's Discovery Boot Camp and for a course on eLitigation. She is currently participating in the Department's Leadership Excellence Achievement Program (LEAP).

Page Intentionally Left Blank

Making it Stick: Protecting Your White Collar Convictions on Appeal

Kelly A. Zusman
Appellate Chief
United States Attorney's Office
District of Oregon

I. Introduction

"Look for the Big Lie." That's the advice veteran white collar prosecutor Claire Fay gives to other Assistant United States Attorneys. That seemingly simple advice is a sound guiding principle for any white collar case. These cases are generally complex, and they involve highly paid, often aggressive defense counsel who will leave no stone unturned. The common tactic: create a dust storm of confusion, blame underlings, express a lack of business acumen and sophistication, and the like. Our most effective response stays true to that simple theme: there was a big lie, and this defendant cannot explain it, hide from it, or ultimately, defend it. He wrote it, said it, posted it, or all three. It was false, it was material, and it formed the backbone of his scheme. Everything else is just white noise. If we stay true to our theme and resist the temptation to run down one of the defense's rabbit holes, we stand a far better chance of success both with the jury and on appeal. In securing the conviction, there are steps we can take to protect our records.

At the outset, although I have defended many white collar convictions on appeal, I am by no means an expert. The lawyers at the Criminal Appellate Division are often called in to assist districts with some of the largest, most complicated white collar cases seen in federal courts. So I consulted with two of those lawyers—David Lieberman and Sonja Ralston—and the advice in this article includes many of their insights. Jefferson Gray, an experienced white collar prosecutor from Maryland, contributed much of the discussion about charging strategies. And because protecting your record for appeal involves all stages of the litigation, we will walk through each phase.

II. Stages of litigation

A. Discovery

Although white collar prosecutors gleefully ignore news from the Supreme Court about the ACCA and its modified, divisible categorical approach, they tend to blanch at the prospect of producing terabytes of information to a defense team that is hell bent on finding something, anything missing. From the Ted Stevens case forward, savvy criminal defense attorneys have defended cases by attacking the prosecution team's failure to deliver discovery. That tactic recently saw success again in the Nevada prosecution of the Bundy family for both crimes of violence and a conspiracy to interfere with federal land management officials. Also, parallel proceedings continue to generate a lot of litigation relative to the prosecution team's discovery obligations. So a few ideas:

(1) If you want to keep your criminal case distinct from a parallel civil proceeding (SEC, EPA, etc.), you must ensure that there is no joint coordination, and that no one from the civil side is telling you what to charge or when to charge it and vice versa. You can share information, but otherwise keep the decision making independent.[1]

(2) Be judicious about what you collect. Your office may be overwhelmed, and the defense may be overwhelmed. Once the material is in our "possession," we are responsible for turning over anything that falls within *Brady-Giglio*, Federal Rules of Criminal Procedure Rule 16, or the Jencks Act.[2] Anything in our indictment, including anything alleged within a conspiracy count, will likely be deemed relevant and material to the defense.[3] In *Bundy*, the court held that the government's failure

---

[1] *See e.g.*, United States v. Blaszczak, 308 F. Supp. 3d 736 (S.D.N.Y. 2018) (finding that although the SEC and United States Attorney's Office conducted 39 witness interviews together, and SEC shared its information with the United States Attorney's Office, the SEC was not part of the prosecution team and, therefore, the prosecution was not obliged to obtain from the SEC its own work product (an "action memo" plus)).

[2] Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972); FED. R. CRIM. P. 16; 18 U.S.C. § 3500.

[3] *See e.g.*, Order Denying Motion for Reconsideration, United States v. Bundy, No. 2:16-cr-00046-GMN-PAL (D. Nev. July 3, 2018), ECF No. 3273.

to disclose evidence related to three of 70 overt acts alleged in the conspiracy indictment justified dismissal of the indictment, with prejudice. Even though the court ruled that self-defense was not available against the government, the court explained that its ruling was based on the absence of evidence (rather than its legal invalidity). Thus, any evidence the government possessed that *might* support self-defense should have been turned over. The court found the discovery violations "flagrant," which then justified dismissal with prejudice.

(3) Document *all* discovery production. The government's failure to do so in a securities trading scheme in *United States v. Chapman* yielded a mid-trial dismissal that the appellate court affirmed.[4]

(4) Although most courts have rejected defense arguments that the government violated discovery obligations by failing to organize or highlight material for the defense, most of those cases have involved instances in which the government provided an index or a list of "hot documents."[5] Although we have no obligation to "help" the defense organize its case, we want our cases to go to trial within a reasonable period of time, and we want the court to have confidence that we are being fair. Sharing some of our organizational work promotes efficiency and serves us well on appeal.

B. Charging

Because white collar cases often involve complex schemes, it is particularly important that our indictment is specific about dates and transactions. Vague allegations are likely to prompt a defense motion

---

[4] United States v. Chapman, 524 F.3d 1073 (9th Cir. 2008).

[5] United States v. Skilling, 554 F.3d 529, 576 (5th Cir. 2009), *aff'd in part, vacated in part,* 561 U.S. 358 (2010) (noting that "the government is under no duty to direct a defendant to exculpatory evidence [of which it is unaware] within a larger mass of disclosed evidence"); *see also* United States v. Lundstrom, 880 F.3d 423, 439 (8th Cir. 2018) (finding no abuse of discretion in denial of defense motion for a bill of particulars because the government provided a list of 400 hot documents and linked each document to the relevant count in the indictment); United States v. Saad, No. 16-CR-035-M-PAS, 2017 WL 888222, at *3 (D.R.I. Mar. 6, 2017), *aff'd,* 888 F.3d 561 (1st Cir. 2018) (denying motion for new trial based on alleged violation of *Brady* in that government failed to highlight in report that an ATF agent improperly stored sample from fire scene in his garage before delivering it to laboratory).

for a bill of particulars, which may be successful if our indictment omits details needed to identify particular transactions.[6] Also, keep in mind that Criminal Justice Act (CJA) funded cases involve the public fisc, so we also want to avoid forcing the defense to expend unnecessary time trying to understand the government's allegations.

In addition to making sure that our indictment allegations are reasonably specific, what follows are highlights for a few white collar charging hotspots.

1. Duplicity

Duplicity is the joining in one count of two or more offenses. The concern raised is that it may be unclear whether the jury agreed on the facts forming the basis for the offense, or jurors may have been confused. Some particular applications:

- *Duplicity* (18 U.S.C. § 1344):[7] An indictment that charges in a single count bank fraud under alternative sections of the bank fraud statute is not duplicitous.[8]

---

[6] *See e.g.*, United States v. Bortnovsky, 820 F.2d 572, 574–75 (2d Cir. 1987) (holding trial court erred in failing to order a bill of particulars; "The Government d[oes] not fulfill its obligation merely by providing mountains of [discovery] to defense counsel who were left unguided as to which documents would be proven falsified or which of some fifteen burglaries would be demonstrated to be staged."); *see also* United States v. Nachamie, 91 F. Supp. 2d 565, 571 (S.D.N.Y. 2000) (granting a bill of particulars in a health care fraud case where the government produced 200,000 pages of records relating to over 2,000 Medicare claims, but failed to inform the defense "which of these claims were false and in what way they were false"); *compare* United States v. Daugherty, No. 5:16-CR-22-DCR-REW, 2017 WL 839472, at *5 (E.D. Ky. Feb. 28, 2017) (no bill of particulars necessary where the government "has told the defense exactly which document categories matter and has identified each suspect medical provider," as well as specifying the allegedly fabricated files); United States v. Dupree, No. 10-CR-627 KAM, 2011 WL 5976006, at *7 (E.D.N.Y. Nov. 29, 2011) (no need for bill of particulars where "[t]he government has been producing documents detailing the allegedly overstated accounts receivable since the day defendants were indicted"); United States v. Hsia, 24 F. Supp. 2d 14, 28 (D.D.C. 1998) (in case involving production of 600,000 pages of discovery, government also produced three notebooks to the defense containing key evidence).

[7] 18 U.S.C. § 1344.

[8] United States v. Crisci, 273 F.3d 235, 239 (2d Cir. 2001).

- *Duplicity* (18 U.S.C. § 1001):[9] An indictment could properly charge a defendant with making a false statement to law enforcement officers and then detail seven separate false statements he made in a particular interview without being duplicitous. However, the jury would need to be instructed at trial that it had to unanimously find that a particular statement or statements were false to return a conviction on that count.[10]

2. Multiplicity

Multiplicity is charging a single offense in multiple counts. An indictment is multiplicitous "when it charges multiple counts for a single offense, producing two penalties for one crime and thus raising double jeopardy questions."[11] There is "no bright line . . . dividing charges comprising a single offense from those comprising separate and distinct offenses."[12] Counts within an indictment are not multiplicitous if each requires proof of an additional fact the other does not.[13] You can cure multiplicity by dismissing or electing to proceed only on certain counts, and because multiplicity is a sentencing concern, dismissal may occur post-trial.

- *Unit of Prosecution/Multiplicity* (18 U.S.C. § 1344):[14] In a bank fraud scheme, unlike in mail and wire fraud, each separate false statement submitted to the bank in furtherance of the scheme is not a separate execution of the scheme that can be charged as a distinct count. Rather, each separate extension of funding by the bank is a punishable act that may be charged as a separate count. Thus, if you submit five different fraudulent documents to a bank at different times in order to get a single large loan that

---

[9] 18 U.S.C. § 1001.
[10] *Crisci*, 273 F.3d at 239.
[11] United States v. Stewart, 420 F.3d 1007, 1012 (9th Cir. 2005); *see also* United States v. Awad, 551 F.3d 930, 937 (9th Cir. 2009) ("An indictment is multiplicitous if it charges a single offense in more than one count.").
[12] United States v. Segall, 833 F.2d 144, 146 (9th Cir. 1987) (citing United States v. Kennedy, 726 F.2d 546, 547 (9th Cir. 1984)).
[13] *Stewart*, 420 F.3d at 1012; *see also* United States v. Garlick, 240 F.3d 789, 793–94 (9th Cir. 2001) ("The test for multiplicity is whether each count 'requires proof of an additional fact which the other does not.'") (citing Blockburger v. United States, 284 U.S. 299, 304 (1932)); *Awad*, 551 F.3d at 937 (quoting the same test from *Garlick*).
[14] 18 U.S.C. § 1344.

is payable all at once, you can charge only a single count violating 18 U.S.C. § 1344.[15]

- *Unit of Prosecution/Multiplicity* (18 U.S.C. § 1001):[16] When identical false statements are made in response to identical questions posed by the same agent, "the declarant may be convicted only once."[17] That is so because "the repetition of a false statement by a declarant does not further impair the operations of the government beyond the initial violation, and a contrary rule would permit the government to pile on multiple convictions by repeatedly asking a declarant the same question."[18] On the other hand, when a defendant "makes two separate false statements to two separate officials, each with distinct duties and functions . . . two convictions under 18 U.S.C. § 1001 are proper," even if the defendant told the same lie to each.[19] A two-part test determines whether false statements may form the basis for separate counts. The first step is to determine whether the defendant "was asked the same question and gave the same answer."[20] The second step examines "whether later false statements further impaired the operations of the government."[21]

3. "On or about" dates

Trying to pin down precisely when a fraudulent scheme began may be impossible. Although our dates need not be precise, and typically involve "on or about" language to permit flexibility, we nevertheless need to ensure that our dates are reasonably accurate; that means the dates should be specific enough to give the defense fair notice, as in "oh, you meant *that* scheme." "[A]n indictment date only needs to be

---

[15] United States v. Lemons, 941 F.2d 309, 318 (5th Cir. 1991) ("In short, the mail and wire fraud statutes punish each act in furtherance, or execution, of the scheme; but the bank fraud statute imposes punishment only for each execution of the scheme."); United States v. Colton, 231 F.3d 890, 908–09 (4th Cir. 2000).

[16] 18 U.S.C. § 1001.

[17] *Stewart*, 420 F.3d at 1013 (citing United States v. Olsowy, 836 F.2d 439, 443 (9th Cir. 1987)).

[18] *Id.*

[19] United States v. Salas-Camacho, 859 F.2d 788, 791 (9th Cir. 1988).

[20] *Id.*

[21] *Id.*

substantially similar to the date established at trial."[22] "[S]ignificant flexibility in proof" is permissible "provided that the defendant was given notice of the 'core of criminality' to be proven at trial."[23] Furthermore, "[p]articularly with respect to allegations of time, we have permitted proof to vary from the indictment provided that the proof fell within the period charged."[24] This is especially true where, as here, time is not an element of the charged offense.[25]

C. Trial-related considerations

1. Evidentiary issues and the Sixth Amendment

The Federal Rules of Evidence apply to the defense, but so does the Sixth Amendment.[26] Although preserved evidentiary objections are reviewed for abuse of discretion, if a trial court's evidentiary rulings effectively exclude a viable defense, it raises a Sixth Amendment concern and the chances of a remand spike significantly. Therefore, resist the temptation to file motions in limine to preclude defense

---

[22] United States v. Teague, 93 F.3d 81, 84 (2d Cir. 1996) (internal quotation and citation omitted).

[23] United States v. Heimann, 705 F.2d 662, 666 (2d Cir. 1983) (citing United States v. Sindona, 636 F.2d 792, 797–98 (2d Cir. 1980)).

[24] *Id.*

[25] *See id.* at 669; s*ee, e.g.*, United States v. Powell, 982 F.2d 1422, 1431 (10th Cir. 1992) (finding a variance between the allegations of conspiracy in the indictment and the evidence presented at trial does not require reversal unless the defendant's substantial rights are affected, and a defendant's substantial rights are not prejudiced "merely because the defendant is convicted upon evidence which tends to show a narrower scheme than that contained in the indictment, provided that the narrower scheme is fully included within the indictment.") (citation omitted); United States v. Laykin, 886 F.2d 1534, 1542–43 (9th Cir. 1989) (finding that because time is not a material element of conspiracy, a variance of about four months between the starting date of a conspiracy as charged and the proof adduced at trial was not reversible error as long as the defendants had adequate notice of the charges against them); United States v. Hathaway, 534 F.2d 386, 401 n.19 (1st Cir. 1976) (finding a variance between the starting date charged and that proven is not fatal if the conspiracy was within the period charged and any discrepancy was insubstantial).

[26] *See* Chambers v. Mississippi, 410 U.S. 284, 302 (1973); *see also* United States v. Mitrovic, 890 F.3d 1217, 1222 (11th Cir. 2018) ("The Federal Rules governing the admissibility of hearsay are neither arbitrary nor disproportionate.").

experts and witnesses without taking a hard, objective look. Ask yourself these questions: (1) What is the defense theory of relevance, and is there any legal support for it; (2) How potentially damaging to my case is this evidence? For example, does it tend to promote jury nullification; (3) Could it be easily neutralized by cross-examination or other evidence; (4) If CJA funds are being used to pay for this witness (for example, experts), is it an affront to the taxpayers or a complete waste of the jury's time?

On the flipside, we also need to be judicious about seeking to admit evidence that raises Federal Rule of Evidence 403 concerns. Remember that the goal is a fair trial in which the jury's focus is on whether the defendant committed the crime charged, not whether the defendant is a good person. For a sobering reminder of just how harsh some of our evidence may look to a three-judge panel presented with nothing but a cold record, see the oral argument from a white collar fraud prosecution against a couple that was already wealthy (before the crime).[27]

2. Summary exhibits

When admitted via Federal Rule of Evidence 1006, these are golden on appeal. As valuable as these tools are to explaining a fraudulent scheme to a jury, they are equally useful on appeal when explaining the case to an intelligent but impatient judicial audience. Charts, exhibits, photographs, and timelines are both visually interesting and highly credible. They permit us to show appellate courts what happened instead of simply telling them and then hoping they believe us after they track down all of our record citations. I cannot stress enough, move to admit these summaries into evidence. Purely "demonstrative" charts and summaries may help with your jury, but they do not help with an appeal since we are limited to evidence properly admitted into the record.[28] See footnote 29 below for some

[27] *See* Oral Argument, United States v. Winston Bontrager, No. 13-30339 (9th Cir. July 9, 2015), https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000007998.

[28] The Seventh Circuit has cautioned against using the term "demonstrative exhibit." A demonstrative aid is a "pedagogical device[] . . . used to aid the jury in its understanding of the evidence that has already been admitted." Baugh *ex rel.* Baugh v. Cuprum S.A. de C.V., 730 F.3d 701, 707 (7th Cir. 2013). Demonstrative aids "illustrate or clarify a party's position" and "they

cases that can be helpful in getting Federal Rule of Evidence 611(a) demonstrative charts admitted into evidence.[29]

3. Jury instructions generally

Although they will not guarantee an affirmance, relying on your circuit's model instructions is your best bet. The key is to ensure that you have the court's latest version of the instruction because they update frequently; consequently, do not print out hard copies for later reference. Always pull from the court's website so you know you have the most current version.

On the flip side, avoid the temptation to propose a particular jury instruction simply because a court in your district used it in a previous case. Context matters. The facts of your case may differ; your defendant may have a separate (or better) objection to raise; or case law may have shifted in the intervening period.

4. Willful blindness (deliberate ignorance) jury instructions

Appellate courts view these instructions with disfavor, so successfully seeking one is a sure-fire way to draw heightened appellate scrutiny to your case. Ask for them if you have a solid record to justify it, but please do so with caution.

A willful blindness instruction is appropriate where "the defendant asserts a lack of guilty knowledge, but the evidence supports an inference of deliberate ignorance."[30] "Ignorance is deliberate if the

---

are by definition less neutral in [their] presentation and thus are not properly considered evidence." *Id.* (internal citations omitted). There is not a requirement that demonstrative aids be "completely accurate." Roland v. Langlois, 945 F.2d 956, 963 (7th Cir. 1991). Instead, the demonstrative aid need only be a fair and accurate depiction of what the witness seeks to describe. *See* United States v. Myers, 972 F.2d 1566, 1579 (11th Cir. 1992) (referencing the fair and accurate standard). Generally, demonstrative aids should be admitted with a limiting instruction. *See* Hinkle v. City of Clarksburg, W. Va., 81 F.3d 416, 424 (4th Cir. 1996); United States v. Cox, 633 F.2d 871, 874 (9th Cir. 1980).

[29] *See* United States v. Johnson, 54 F.3d 1150, 1158–59 (4th Cir. 1995); United States v. Pinto, 850 F.2d 927, 935–36 (2d Cir. 1988); United States v. Stephens, 779 F.2d 232, 239 (5th Cir. 1985); United States v. Gold, 743 F.2d 800, 816 (11th Cir. 1984).

[30] United States v. Whitehill, 532 F.3d 746, 751 (8th Cir. 2008) (citing United States v. Gruenberg, 989 F.2d 971, 974 (8th Cir. 1993)).

defendant[] w[as] presented with facts putting [him] on notice criminal activity was particularly likely and yet intentionally failed to investigate."[31] Such an instruction is not, however, proper when the evidence demonstrates only that defendant either possessed or lacked actual knowledge of the fact in question.[32] The court's concern is that it does not want a jury premising criminal liability on negligence.

Other courts have adopted similar, fairly stringent evidentiary requirements to justify the instruction—requiring proof that a defendant affirmatively did *something* to avoid actual knowledge.[33]

5. Build a team

Sufficient staffing is crucial when it comes to complex white collar fraud cases. Trial counsel may well need what I refer to as a "pit crew." Recruit folks from appellate or other Assistant United States Attorneys known for their writing skills to help respond to the prolific, often late-night motions that require speedy but thoughtful responses. Trying to do too much yourself will wear you down and it could ultimately hurt your case. Appellate Assistant United States Attorneys can help with everything from charging decisions, evidentiary issues, jury instructions, motions in limine, and trial memoranda. Sometimes, just having a fresh set of eyes can save your case from disaster.

Also, do not be afraid to seek guidance from your Appellate Chief or the Criminal Appellate Section when you spot a novel legal issue on the horizon. These consultations can minimize, or even neutralize, the risk of appellate reversal. Remember that we are part of an even larger team—93 United States Attorneys' Offices plus our colleagues at Main Justice. Chances are that a prosecutor in the Department has already encountered the same issue. Never pass up a chance to reach out to an experienced colleague in another office for advice.

---

[31] *Id.*

[32] United States v. Barnhart, 979 F.2d 647, 651–52 (8th Cir. 1992).

[33] *See e.g.*, United States v. Scott, 159 F.3d 916, 922 (5th Cir. 1998) (requiring proof that (1) defendant was substantially aware of a high probability of the existence of illegal conduct; and (2) the defendant purposely contrived to avoid learning of the illegal conduct); United States v. Mapelli, 971 F.2d 284, 286 (9th Cir. 1992) (requiring proof that defendant "purposely contrives to avoid learning all the facts"); United States v. de Francisco-Lopez, 939 F.2d 1405, 1409 (10th Cir. 1991) (observing that the instruction is "rarely appropriate" and finding reversible error because the acts relied on to infer knowledge must be "deliberate" and "not equivocal").

For example, during a recent bank fraud trial in Oregon, a spectator sitting in the back of the courtroom violated Federal Rule of Evidence 615 when he emailed detailed daily testimony summaries to an upcoming defense witness despite a witness exclusion order. Although the understandable reaction was to seek to preclude the defense witnesses' testimony altogether, some quick research by the pit crew unearthed a Ninth Circuit ruling suggesting it was error to preclude a defense witness unless there was proof that the defendant or his legal team was actually behind the Rule 615 breach.[34] So instead of seeking to exclude the witness, our trial team effectively cross-examined the witness about the spectator's email messages.

6. Exercise caution and restraint during closing argument

According to a study conducted by a jury consulting firm, nearly 80% of cases are decided by the jury after opening statements. What does that tell you about the risks we should be taking during closing argument? Particularly, our rebuttal arguments tend to be unscripted and incited by the defense's fiery rhetoric. Although the courts recognize that prosecutors may strike "hard blows," heavy hitting may prompt greater appellate scrutiny.[35]

For white collar prosecutors, there are three primary danger zones. The first involves "send a message" arguments—that is, those that encourage a verdict on a deterrence rationale rather than the

[34] There are generally three recognized remedies for a violation of a witness sequestration order under Rule 615: (1) hold the witness in contempt; (2) permit cross-examination on the 615 violation; or (3) preclude the witness's testimony altogether. *See* United States v. Hobbs, 31 F.3d 918, 921 (9th Cir. 1994) (citing Holder v. United States, 150 U.S. 91, 92 (1893)). The Ninth Circuit, like most other circuits, has described disqualification as a remedy that should be "used sparingly," and observed that it is "strongly disfavored." *Id.* at 921; United States v. Erickson, 75 F.3d 470, 480 (9th Cir. 1996); *see also* United States v. Cornell, 780 F.3d 616, 628 (4th Cir. 2015). Indeed, the "usual remedy" is simply to allow the aggrieved party to ask the witness about the Rule 615 violation on cross-examination. *Erickson*, 75 F.3d at 480. Courts generally view this remedy as an effective "cure" for any Rule 615 violation. United States v. Cozzetti, 441 F.2d 344, 350 (9th Cir. 1971).

[35] United States v. Sullivan, 522 F.3d 967, 982 (9th Cir. 2008).

evidence.[36] The second relates to generalizations that may be mostly, but not entirely, accurate.[37] Finally, can you call the defendant a liar? The circuits are split, but at least two have expressed a preference for references to "lies" rather than labels like "liar."[38] Regardless of how you approach this, be mindful of our ethical obligation not to express a personal opinion about a defendant's guilt.[39]

D. Post-trial considerations

1. Preservation

Has your defendant raised claims or arguments for the first time in his Federal Rule of Criminal Procedure 33 motion for a new trial? If so, argue that he failed to preserve the point. We often raise preservation objections on appeal, but it is equally important to raise them in district court too so that you afford your trial judge the opportunity to weigh in. Preservation is a particularly important doctrine for trial judges because it requires that lawyers raise specific objections at trial to give the judge fair notice and a reasonable opportunity to do the right thing. Late, after-the-fact arguments should be unsuccessful unless the error was blatant (that is, "plain"). It puts us in a better position on appeal if we can point to a trial court's ruling that an argument was not properly preserved.

2. Sentencing

In large fraud cases, sentencing often turns into the main event, eclipsing the trial in duration and significance. The most common issue seen in appeals from sentencing for white collar cases involves loss computations. Because fraudsters are so creative, the sentencing guidelines often seem a difficult fit for particular cases. The U.S.

---

[36] *See e.g.*, United States v. Certified Envtl. Servs., Inc., 753 F.3d 72 (2d Cir. 2014) (reversing a conviction for cumulative errors, including improper closing argument; "CES is still in business . . . your verdict is going to have consequences. . . .").

[37] *See e.g.*, United States v. Reyes, 577 F.3d 1069 (9th Cir. 2009) (not everyone was in the dark about back dated stock transactions);
United States v. Womack, 481 F. App'x 925 (5th Cir. 2012) (proof at trial related to 25 false tax returns and did not establish that the entire business was fraudulent).

[38] United States v. Phillips, 704 F.3d 754 (9th Cir. 2012);
United States v. Poole, 735 F.3d 269, 277 (5th Cir. 2013).

[39] *See* MODEL RULES OF PROF'L CONDUCT r. 3.4 (AM. BAR ASS'N 2015).

Sentencing Commission has a helpful monograph covering fraud loss litigation issues, and that tends to be my first stop.[40]

Fraud loss for guideline purposes, distinguished from the more circumscribed losses for restitution, can be a rougher estimate and may include intended but unrealized losses.[41] Further, if actual or intended loss is too difficult to discern, a court may instead look to a defendant's gain.[42] Courts interpreting this guideline provision have emphasized its flexible and pragmatic approach. Losses for guideline purposes—unlike restitution or civil damage awards—may be imprecise estimates because they serve only to set the offense's relative scale.[43]

District judges are afforded a wide degree of discretion to tailor loss methods to suit particular cases.[44] A sentencing judge need not find a perfect fit between the loss figure and the method used to reach it: "[T]here exists no rigid formula for the sentencing court to follow in attempting to determine the victim's loss in fraud cases when the amount of neither actual nor intended loss is readily apparent."[45] We may, however, need to recognize offsets when a defendant actually delivers something of value.[46] Keep in mind that many guideline disputes are, at bottom, factual disputes. When the defendant challenges a loss calculation or an offense-level enhancement, we need to confirm that we have assembled an adequate record to support our

---

[40] U.S. SENTENCING COMM'N, PRIMER ON LOSS CALCULATIONS UNDER § 2B1.1(b)(1) (April 2017).

[41] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(A) (U.S. SENTENCING COMM'N 2004).

[42] *See, e.g.*, United States v. Martinez, 690 F.3d 1083, 1088 (8th Cir. 2012).

[43] *See, e.g.*, United States v. Tadios, 822 F.3d 501, 503 (9th Cir. 2016) (referencing U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(C) (U.S. SENTENCING COMM'N 2004)).

[44] *See e.g.*, United States v. Bussell, 504 F.3d 956, 961–62 (9th Cir. 2007) ("declin[ing] to impose a mechanical limitation on intended loss" and refusing to "tie the sentencing court's hands").

[45] United States v. W. Coast Aluminum Heat Treating Co., 265 F.3d 986, 991 (9th Cir. 2001).

[46] *See e.g.*, United States v. Martin, 796 F.3d 1101 (9th Cir. 2015) (remanding for reconsideration with directions to give credit to any legitimate service rendered to victims where defendant constructed guardrails as promised, but misrepresented her finances to secure a government contract as a disadvantaged business).

preferred outcome and that the district court has provided an adequate explanation to justify its ruling.[47]

My final advice for sentencing is to be like Claire Fay. She is one of the most thorough and meticulous Assistant United States Attorneys I know. She routinely dives into defense haystacks and finds the needles, which she then uses to stitch together their sentencing shroud. Securing lengthy sentences in white collar cases is, as most of you know, a daunting prospect because many of our defendants have no prior criminal history and a lot of local family and community support. Ensuring that the court begins its sentencing analysis with a complete and accurate guideline computation that takes into account all applicable enhancements gives us a strong starting position.

III. Concluding thoughts

In addition to all of the highlights covered in this article, white collar fraud cases are also distinctive because they frequently involve large numbers of victims. Many victims continue to track cases as they work their way through an appeal, and I have seen and heard from victims who remain concerned that a defendant who scammed them will be released or some way relieved of his sentence or restitution obligation. Some dread the prospect of having to retake the witness stand if the case is sent back for a new trial. Consequently, keeping your victim witness coordinators apprised of the case's progress is important, as is explaining the appellate and post-conviction process. Winning convictions is important, and preserving them on appeal, particularly when they involve victims hoping to recoup restitution, is equally important. Make it stick.

About the Author

Kelly A. Zusman is the Appellate Chief for the United States Attorney's Office in Oregon. Prior to joining the Department, she served as a law clerk to U.S. District Court Judge Malcolm F. Marsh, and Ninth Circuit Judge Otto R. Skopil. She has worked as a Civil Assistant United States Attorney, a Criminal Assistant United States Attorney prosecuting violent crimes, and she previously served as her office's Senior Litigation Counsel. Zusman teaches legal research and writing, appellate advocacy, trial advocacy, evidence, and criminal

[47] *See* United States v. Prange, 771 F.3d 17, 36–37 (1st Cir. 2014) (remanding for resentencing because the district court failed to make factual findings supporting its conclusion that the returned stock was worthless).

discovery for the National Advocacy Center, Main Justice, and United States Attorneys' Offices throughout the country. She is also an adjunct professor for the University of Oregon and the Northwestern School of Law, teaching evidence, appellate advocacy, and criminal investigations. She is the author of OLE's "Federal Appellate Advocacy" Handbook, a chapter in the Blue Book on Criminal Discovery, a chapter in the Blue Book on Trial Practice, and she maintains and updates the Brady/Giglio and Federal Privileges outlines. In 2013 and 2018, she received EOUSA Director Awards for Outstanding Appellate Advocacy.

Page Intentionally Left Blank

A Shot in the Dark: Using Asset Forfeiture Tools to Identify and Restrain Criminals' Cryptocurrency

Shirley U. Emehelu
Chief, Asset Recovery and Money Laundering Unit
United States Attorney's Office
District of New Jersey

I. Introduction

Over the past decade, law enforcement has witnessed a rise in the use of various forms of cryptocurrency in wide ranging types of criminal enterprises—including drug trafficking, child exploitation, human trafficking, financial fraud, and money laundering schemes, to name just a few. Cryptocurrency offers many benefits to those engaged in criminal activities including anonymized payment transactions; the elimination of the need to transport bulky quantities of cash to fund and launder the proceeds of criminal activity; a transnational form of currency that can be used globally; the ability to engage in speculation arising from potential spikes in the value of cryptocurrency; and relatively low financial regulation compared to heavily regulated forms of traditional currency. This article demonstrates the impactful role that asset forfeiture can play in effectively investigating and prosecuting crimes involving cryptocurrency.

A. The advantages of asset forfeiture

Asset forfeiture is an integral part of federal criminal law enforcement. It can serve as a powerful tool in cases involving cryptocurrency as the spoils of the crime or the currency driving the crime.

In this area (as in many others), a number of critical objectives are achieved through asset forfeiture. Asset forfeiture removes the instrumentalities of crime from the control of wrongdoers. Such instrumentalities may include cryptocurrency, which, although not illegal in and of itself, can provide criminals the ability to fund criminal schemes and launder the proceeds thereof with relative anonymity. In addition, asset forfeiture is a crucial mechanism for

recovering assets that may be used to compensate innocent victims in cases involving property offenses and fraud. In such cases, asset forfeiture allows for the preservation of assets, such as cryptocurrency, during the pendency of the criminal case so that the assets can be liquidated and the funds restored to victims for restitution.[1]

Asset forfeiture also takes the profit out of crime by removing the fruits of illegal crimes—such as cryptocurrency—from the hands of wrongdoers. This sends a deterrent message to those contemplating engaging in economic crime by increasing the risk that a criminal will be stripped of his ill-gotten gains. Finally, asset forfeiture serves as a form of punishment by depriving a convicted wrongdoer of the assets that provided the wrongdoer the means with which to commit the criminal activity and the spoils that came with accomplishing the criminal scheme.

In order to be able to realize these important objectives, there first must be statutory grounds to pursue asset forfeiture in a given case. For example, there may be statutory authority to seize cryptocurrency as the proceeds of the criminal offense;[2] the payment source used or intended to be used to purchase a controlled substance;[3] property involved in a money laundering offense;[4] property acquired or maintained through racketeering activity;[5] or the property of an individual engaged in planning or committing acts of domestic or

---

[1] *See* 18 U.S.C. § 981(e)(6) (authorizing the government, in civil forfeiture cases, to use forfeited property to pay restitution to the victims of the underlying crimes); 21 U.S.C. § 853(i) (authorizing the same for criminal forfeiture).

[2] *See, e.g.*, § 981(a)(1)(C) (authorizing the forfeiture of the proceeds of a long list of state and federal crimes, including fraud, bribery, embezzlement, and theft); § 853(a)(1) (outlining property subject to criminal forfeiture); 21 U.S.C. § 881(a)(6) (authorizing the forfeiture of the proceeds of drug offenses).

[3] *See* § 881(a)(6) (subjecting to forfeiture, inter alia, all moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance, and all proceeds traceable to such an exchange).

[4] *See* § 981(a)(1)(A) (civil forfeiture); 18 U.S.C. § 982(a)(1) (criminal forfeiture).

[5] *See* 18 U.S.C. § 1963(a).

international terrorism, regardless of whether the cryptocurrency was involved in the terrorism activity.[6]

As set forth below, identifying and seizing forfeitable cryptocurrency requires careful planning by prosecutors and their law enforcement partners.

B. Cryptocurrency terms

Before discussing law enforcement techniques for identifying and seizing cryptocurrency, it is important first to understand certain key concepts related to cryptocurrency.

1. Centralized vs. decentralized digital currency

Cryptocurrency, also known as "digital currency" or "virtual currency," is generally defined as "a digital unit of exchange that is not backed by a government-issued legal tender."[7] The first digital currencies were "centralized," meaning that they were controlled by centralized, private entities.[8] A few examples of these early, centralized digital currencies were E-gold, a digital currency purportedly backed by gold bullion, and Liberty Reserve, an online payment system in which users transacted in digital currency.[9] Both E-gold and Liberty Reserve ultimately were prosecuted and/or shut down by law enforcement for facilitating wide scale money laundering.[10]

---

[6] *See* § 981(a)(1)(G) (conferring extremely broad forfeiture authority that allows the government to seize and forfeit *all* assets, foreign or domestic, of a terrorism defendant).

[7] *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks* at 3 (U.S. GOVERNMENT ACCOUNTABILITY OFFICE May 2013) [hereinafter GAO REPORT].

[8] Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13, at *5 (2014).

[9] *Id*.

[10] In July 2008, E-Gold Ltd. (E-Gold), its corporate affiliate Gold & Silver Reserve Inc., and its three principal directors and owners—Douglas Jackson, Barry Downey, and Reid Jackson—pled guilty to criminal charges relating to money laundering and the operation of an illegal money transmitting business. *See* Press Release, U.S. Dep't of Justice, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges (July 21, 2008). As for Liberty Reserve, law enforcement shut down the digital currency payment system in May 2013, as it had grown into a financial hub for criminal actors around the world, who used it "to amass,

In contrast, "decentralized" digital currencies "have no centralized administrating authority and instead operate as peer-to-peer transaction networks[.]"[11] Bitcoin, the first decentralized cryptocurrency emerged around 2009. Bitcoin remains the world's most widely used virtual currency. Several other cryptocurrencies have emerged, such as Monero, Ethereum, Dash, and Litecoin.[12]

Figure 1: Cryptocurrencies and Respective Icons

2. Blockchain transactions

Using a peer-to-peer network, an owner of Bitcoin or other similar cryptocurrency may make an online payment to another party without going through a financial institution. Unlike traditional or "fiat" currencies, cryptocurrencies are not minted or printed by a central government or agency. Instead, cryptocurrencies like Bitcoin are "mined" by "miners," members of the cryptocurrency network who offer their computers' processing power to solve mathematical

---

distribute, store, and launder criminal proceeds of their [online Ponzi schemes], including proceeds of investment fraud, credit card fraud, identity theft, and computer hacking." Press Release, U.S. Dep't of Justice, Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million (Jan. 29, 2016). By the time it was shut down, Liberty Reserve had five million user accounts worldwide, including more than 600,000 accounts associated with users in the United States, and had processed millions of transactions. *Id.* In January 2016, Arthur Budovsky, the founder and operator of Liberty Reserve, pled guilty in federal court to conspiring to commit money laundering, admitting that he had laundered between $250 million and $550 million in criminal proceeds linked to Liberty Reserve accounts based in the United States. *Id.* Budovksy was sentenced, in May 2016, to 20 years in prison for his massive money laundering enterprise. *See* Press Release, U.S. Dep't of Justice, Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court (May 6, 2016).

[11] Trautman, *supra* note 8, at *5 (citation omitted).

[12] Alex Hern, *Everything You Wanted to Know About Bitcoin But Were Afraid to Ask*, THE GUARDIAN, Nov. 11, 2017.

equations confirming that the sender of funds in each transaction has the right to spend the specific cryptocurrency involved. This mining process yields a general ledger of transactions that are publicly accessible on the Internet. This publicly available ledger is called "blockchain"—a list, or "block," of transactions that are made during a set period of time that includes the unique hash for each block. [13] "A 'hash' is a unique random sequence of letters and numbers that is shorthand for a unique transaction between users that is stored with the block."[14] The blockchain prevents an individual from using already spent cryptocurrency to transact with someone else. Each new block incorporates the prior block's hash.[15]

3. Public vs. private key

There are two important components of cryptocurrency transactions: the "public key" and the "private key." A public key or public address, which may be thought of as a bank account number, is shared by a Bitcoin[16] user with other individuals from whom the user would like to receive Bitcoin payment. The private key, which is akin to an ATM pin number, enables the user to send or spend Bitcoin from his or her Bitcoin wallet.[17]

The publically accessible blockchain, which evidences the validation and settling of cryptocurrency transactions, does not identify the users' actual names, personal identifying information, or their private keys. The blockchain does, however, include the Bitcoin address, or public key, of the sending and receiving parties, the amount of the transaction, IP addresses, the date and time of the transaction, and other information.[18]

4. Cryptocurrency wallets

Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive

---

[13] Christopher Burks, *Bitcoin: Breaking Bad or Breaking Barriers?,* 18 N.C. J. L. & TECH. 244, 248–49 (2017).
[14] *Id*. at 249 n.18.
[15] *Id.* at 249.
[16] Although there are now many forms of cryptocurrency, Bitcoin will predominantly be referred to here, given that it is the most commonly used type of cryptocurrency.
[17] *A Beginner's Guide to Blockchain Technology*, COINDESK, https://www.coindesk.com/information/.
[18] *Id*.

cryptocurrency. There are a plethora of different types of wallets, which offer varying levels of, among other things, value, convenience, risk of loss, and anonymity. Whoever possesses the private key has unrestricted access to the cryptocurrency in the wallet. Without the private key, access to the cryptocurrency cannot be obtained.[19]

Some wallets are browser-based, meaning that they are hosted and serviced by providers via the Internet. Alternatively, a software client downloaded on a user's computer can be used to access a wallet, or users may access wallets via a mobile device or smartphone by downloading an application from a wallet provider.[20]

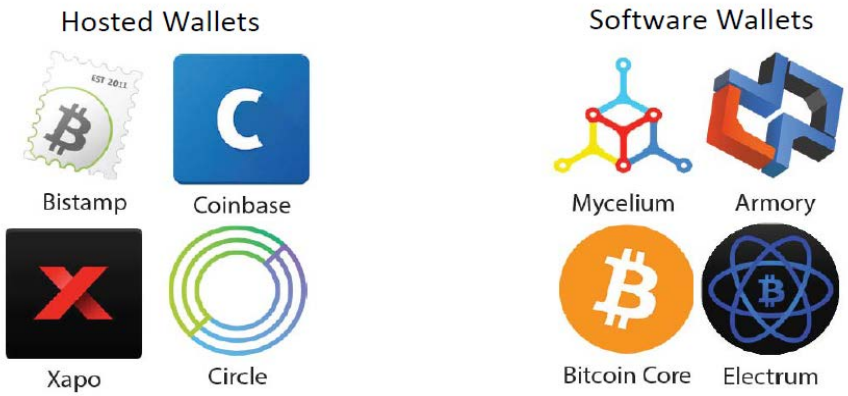

Figure 2: Examples of Cryptocurrency Wallets

[19] *Id.*
[20] *Id.*

Figure 3: Icons Depicting Various Wallet Programs

A user may also effect cryptocurrency transactions by sharing a public key or address with other users via a Quick Response (QR) Code, which is a barcode that can be scanned by technologies available on many smartphones and other devices.[21]

Wallets themselves come in different forms—for example, a paper wallet is simply the user's private and public key memorialized on paper. Alternatively, a user can obtain a physical coin that is preloaded with the value of the cryptocurrency. With a brain wallet, the user's private key is encrypted into a phrase for the user to recall through the use of third party software that generates a phrase associated with a private key. Finally, a "cold storage" wallet stores the cryptocurrency offline, for example on a hardware device.[22]

[21] *Id.*
[22] *Id.*

Figure 4: Forms of Wallets for Cryptocurrency

5. Cryptocurrency exchanges

A cryptocurrency exchange provides customers the ability to buy and sell cryptocurrency using traditional currency—transacting either with the exchange or among themselves—and the exchange also may allow a customer to exchange one type of cryptocurrency for another (for example, exchanging Bitcoin for Monero).[23]

6. The dark web

The "dark web" is a portion of the "Deep Web" of the Internet, where individuals must use an anonymizing software of application called a "darknet" to access content and websites. The Deep Web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items—often with cryptocurrency as the preferred method of payment—such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring.[24] Famous dark web marketplaces such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law

[23] *Id.*

[24] *See generally* DANIEL SUI, ET AL., WILSON CENTER, SCI. & TECH. INNOVATION PROGRAM, THE DEEP WEB AND THE DARKNET: A LOOK INSIDE THE INTERNET'S MASSIVE BLACK BOX (Aug. 2015).

enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

The "Tor network" or simply "Tor" (an abbreviation of "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol (IP) addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network.[25]

II. Forfeiting cryptocurrency

With key terms defined, we can now discuss the investigative mechanics of identifying and seizing forfeitable cryptocurrency. A comprehensive seizure plan is critical to ensuring the seamless identification, seizure, preservation, and liquidation of forfeitable cryptocurrency.

A. Identifying cryptocurrency transactions

The determination of whether a subject is transacting in cryptocurrency in connection with a criminal scheme is often made during the investigative stage, through the review of financial records of the subject. This financial records review may reveal transactions with cryptocurrency service providers such as cryptocurrency exchangers, payment processors, and wallet providers. Once particular cryptocurrency service providers are identified from financial records, those third-party service providers can be subpoenaed for customer account records, which may help identify suspicious cryptocurrency transactions involving the subject.

The open-source nature of blockchain transactions also facilitates an investigator's determination of whether a criminal subject has transacted in cryptocurrency. There are various online tools, called blockchain or block "explorers," that are publicly available on the Internet that enable one to search the data contained in the blockchain. Thus, for example, if an investigator learns of a Bitcoin address associated with a particular scheme, the investigator can search the address through a blockchain explorer in order to locate possible Bitcoin transactions involving that particular address. The block explorer search can reveal the following transactional

[25] *Id.*

information: the Bitcoin transaction ID and Date/Time Stamp (in Universal Coordinated Time/UTC), the amount of Bitcoin (BTC) transacted, the sender's public key or Bitcoin address, and the receiver's public key or Bitcoin address. IP address information may also be revealed, but the IP addresses may not be the true locations of the Bitcoin senders and receivers, because many exchangers and wallet providers may use proxy IPs or IPs that do not constitute the true location of the computer or device used to access the Bitcoin network to carry out the transaction. That being said, if an investigator is aware of a particular IP address utilized by a subject, the investigator can use that IP address to execute a search using the block explorer online tool to identify any cryptocurrency transactions executed using that IP address.

Once a suspicious cryptocurrency transaction has been identified, and if it is determined that the transaction was effected through a cryptocurrency payment processor, a subpoena can be issued to the payment processor requesting, among other things, any wallet address(es) associated with the transaction, any bank account number(s) registered to the user, and any personal information linked to the account user (for example, name, email, address, phone number, IP logs, and credit card information).

Court-issued search warrants for email and text message content stored by third party electronic service providers also can yield information related to a subject's engagement in cryptocurrency transactions. Such records may reveal communications with cryptocurrency exchanges, wallet-service providers, individuals desirous of engaging in cryptocurrency transactions, and other evidence of cryptocurrency usage.

Law enforcement review of communications and contraband trafficking on Darknet markets or websites can also produce valuable information regarding a subject's cryptocurrency usage, since cryptocurrency is generally the currency of choice for criminals on the Darknet.

B. Seizure of cryptocurrency

Thus far, we have discussed some covert methods for obtaining information regarding a criminal subject's engagement in cryptocurrency transactions. Next, we will discuss how to prepare for the overt stage of an investigation in light of a criminal subject's cryptocurrency usage, so that said cryptocurrency can be effectively seized and preserved during the pendency of the criminal case.

The central objective for seizing cryptocurrency that was stolen or used to facilitate criminal activities is gaining access to a subject's private key. The private key may be controlled by (1) a wallet installed on the subject's computer, smartphone, or an external storage device such as a hardware wallet or a USB drive; (2) a paper wallet or memorialized on a piece of paper; and/or (3) a third party such as a cryptocurrency exchanger or online wallet provider. Therefore, court-issued search warrants for the subject's residence, business, cellular telephone, and person should include wallets and evidence of the private key among the items to be seized. Forfeiture seizure warrants, court-issued pursuant to 18 U.S.C. §§ 981(b) and 982(b), 21 U.S.C. § 853(f), and 21 U.S.C. § 881(b), may be served on third-party custodians of a subject's cryptocurrency such as exchangers and online wallets if the cryptocurrency is statutorily subject to forfeiture based on the criminal offense or offenses that the subject is suspected of committing.

The investigator's job is not complete with the recovery of the subject's private key data, since the subject or an associate with access to the private key can simply move the cryptocurrency to another address. The investigator must be readily prepared to transfer the cryptocurrency into a secure wallet controlled by law enforcement. Thus, effective seizure planning will require that law enforcement wallet(s) be in place prior to seizure, and the address(es) for the wallet(s) should be readily accessible to law enforcement so that the subject's cryptocurrency can be transferred without delay on the day of the takedown. This is particularly important where the subject's cryptocurrency wallets are encrypted, which may require exporting the private keys from the subject's computer or device while it is online and running.

Law enforcement interviews of subjects should include in-depth questioning regarding the subject's cryptocurrency usage, including but not limited to the types of wallets, payment processors, and/or exchangers used by the subject, the location of wallets, private key information, and passwords for encrypted wallets.

Prosecutors moving to compel a defendant to disclose his or her encryption password or private key face litigation risk, since there is a dearth of case law dealing with compelled decryption. There do not appear to be any reported cases dealing with compelled disclosure of cryptocurrency private keys, and the holdings of the cases that do address compelled decryption are contradictory. In what appears to be the earliest reported case addressing the constitutionality of

compelled decryption, the government sought to decrypt the Z-drive of the defendant's laptop, the contents of which the defendant had allowed an agent to search before the defendant's arrest for knowing transportation of child pornography and the seizure of the laptop, which was shut down after seizure.[26] A search warrant was obtained for the laptop, but during the course of creating a mirror image of its contents, the government discovered that it could not find or open the Z-drive. A grand jury subpoena was issued directing the defendant to produce the password, and the defendant moved to quash the subpoena. During oral argument and in post-argument submissions, the government stated that it intended only to require the defendant to provide an unencrypted version of the drive to the grand jury, in lieu of the password itself.

In adjudicating the defendant's motion to quash, the court considered the United States Supreme Court's holdings in several other cases to determine the central question: "whether requiring Boucher to produce an unencrypted version of his laptop's Z drive would constitute compelled testimonial communication."[27] Applying the "foregone conclusion" doctrine,[28] the court in *Boucher* concluded that compelling decryption did not constitute compelled testimonial communication because the government previously knew the location of the Z-drive and its files since the defendant allowed the agent to view the contents of the Z-drive, upon which the agent determined that it appeared to contain images or videos of child pornography.[29] Thus, the court reasoned, the defendant's act of producing an unencrypted version of the Z drive was not necessary to authenticate it because he already admitted to possessing the computer and provided the government with access to the Z drive.[30] Since *Boucher* was decided, courts have reached mixed holdings.[31]

---

[26] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

[27] *Id.* at *3 (considering Fisher v. United States, 425 U.S. 391 (1976), United States v. Doe, 465 U.S. 605 (1984), Doe v. United States, 487 U.S. 201 (1988), and United States v. Hubbell, 530 U.S. 27 (2000)).

[28] *See Fisher*, 425 U.S. at 411.

[29] *In re Boucher*, 2009 WL 424718, at *4.

[30] *See id.*

[31] *See, e.g.,* United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (quashing a subpoena ordering the defendant to provide all passwords associated with computer and any files on it based on court's finding that providing the government access to his encrypted files would violate his

C. Establishing the forfeitability of seized cryptocurrency

Seized cryptocurrency is maintained in the custody of the U.S. Marshals Service in secure wallet(s) pending the resolution of the criminal case and the adjudication of the cryptocurrency's forfeitability, which is determined in accordance with the same procedural rules that govern the adjudication of the forfeitability of any form of specific property in a criminal case.

Criminal forfeiture procedure is discussed herein, but the government may seek civil forfeiture in parallel with, or in lieu of, criminal forfeiture. In a civil forfeiture case, the government files a civil action in rem against the property itself, and must prove by a preponderance of the evidence that the property was derived from or was used to commit a crime. Thus, unlike criminal forfeiture, civil forfeiture does not depend on a criminal conviction and civil forfeiture may proceed even if the defendant property belongs to a fugitive, someone who has died, or where the government can prove that the property was involved in a crime but cannot identify the wrongdoer.[32]

---

privilege against self-incrimination); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012) (holding the Fifth Amendment privilege was not applicable where defendant declined to produce the unencrypted contents of her laptop, since the contents of the laptop and facts communicated by the production of those contents were foregone conclusions, where the government knew of the existence and location of the computer's files, notwithstanding the government's lack of knowledge as to the specific contents of said files); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012) (reversing district court's contempt holding for defendant's refusal on Fifth Amendment grounds to comply with a subpoena requiring defendant to appear before a grand jury and produce the unencrypted contents of his hard drives, and rejecting the foregone conclusion argument given that the government's mere possession of the hard drives did not mean it knew of the existence and location of the electronic files stored therein, and because the decryption and production of the contents of the hard drives would form a link in the chain of evidence that would lead to incriminating evidence).

[32] *See, e.g.*, United States v. One-Sixth Share Of James J. Bulger In All Present And Future Proceeds Of Mass Millions Lottery Ticket No. M246233, 326 F.3d 36, 40 (1st Cir. 2003) ("Because civil forfeiture is an in rem proceeding, the property subject to forfeiture is the defendant. Thus, defenses against the forfeiture can be brought only by third parties, who must intervene.").

Procedurally, civil forfeiture actions are closely akin to other civil cases. They commence with a verified complaint filed by the government as plaintiff; claimants are then required to file claims to the property and answer the complaint within a certain period of time; followed by civil discovery, motions practice, and trial—by jury if the right is asserted by a claimant with standing—with the government bearing the burden of establishing the forfeitability of the property by a preponderance of the evidence.[33]

1. Forfeiture allegations in charging document

At the start of the criminal case, the indictment or information must include forfeiture allegations providing notice to the defendant that the government will seek the forfeiture of property as part of any sentence in accordance with the applicable forfeiture statute.[34] The forfeiture allegation should list any property believed to be subject to forfeiture that "includes but is not limited to,"[35] specifically itemized property such as cryptocurrency.

2. Guilty plea convictions

Forfeiture is not judicially adjudicated until after the defendant has been convicted of an offense or offenses supporting forfeiture. If the conviction is by guilty plea, the plea agreement should include forfeiture language setting forth the defendant's agreement to the entry of any forfeiture money judgment and the forfeiture of specific property such as cryptocurrency. The prosecutor should also submit a preliminary order of forfeiture to the court for entry at the plea hearing or shortly thereafter. The preliminary order of forfeiture mirrors the forfeiture stipulations in the plea agreement, setting forth the amount of any forfeiture money judgment and directing the forfeiture of specific property, which would include any forfeitable cryptocurrency.[36]

3. Bifurcated trial procedures

If the defendant elects to go to trial, the court conducts the "forfeiture phase" as part of a bifurcated trial, whereby the "guilt

---

[33] *See generally* 18 U.S.C. § 983; FED. R. CIV. P., SUPP. R. G.
[34] *See* FED. R. CRIM. P. 7(c)(2); FED. R. CRIM. P. 32.2(a).
[35] Using this language allows the prosecutor to later add newly discovered property via a bill of particulars, without superseding the indictment.
[36] *See* FED. R. CRIM. P. 32.2(b)(2).

phase" of the trial is first held and the jury determines whether the defendant is guilty of the underlying criminal charges. If the jury returns a guilty verdict, either side (the government or the defendant) must make a specific and timely request to have the forfeiture phase go before the jury; otherwise, the court will adjudicate the forfeiture phase of the trial.[37] The trier-of-fact (whether the court or the jury) then must determine whether the government has established by a preponderance of the evidence that there is a "nexus" between the specific property that the government seeks to forfeit (for example, cryptocurrency), and the offense(s) of conviction.[38] The trier-of-fact may consider evidence already in the record—whether, for example, from the guilt phase of a trial or in a written plea agreement of a co-defendant—or made after an evidentiary hearing.[39]

If the government seeks a personal money judgment for the amount of proceeds personally obtained by the defendant from the criminal conduct supporting forfeiture, or the value of funds involved in a charged money laundering offense, "the court must determine the amount of money that the defendant will be ordered to pay."[40] Once the forfeiture phase is concluded and the trier-of-fact determines that property and/or any amount of money is subject to forfeiture, the court must promptly enter a preliminary order of forfeiture setting forth the amount of any money judgment and/or directing the forfeiture of specific property, which could include cryptocurrency.[41]

4. Substitute assets

A major advantage of criminal (as opposed to civil) forfeiture is that the government may seek to forfeit "substitute assets" (legitimate assets of a defendant that are equivalent in value to the directly

---

[37] FED. R. CRIM. P. 32.2(b)(4).

[38] *See, e.g.*, United States v. Garcia-Guizar, 160 F.d 511, 518 (9th Cir. 1998); *see also* FED. R. CRIM. P. 32.2(b)(1).

[39] FED. R. CRIM. P. 32.2(b)(1).

[40] FED. R. CRIM. P. 32.2(b)(1)(A). Courts are split as to whether Rule 32.2(b)(4) provides a defendant the right to a jury trial regarding the amount of a money judgment. *Compare* United States v. Tedder, 403 F.3d 836, 841 (7th Cir. 2005) (finding no right to jury trial for determination of amount of money judgment), *with* United States v. Armstrong, No. CRIM 05-130, 2007 WL 809508, at *4 (E.D. La. Mar. 14, 2007) (overruling defense objection to government request for jury trial on amount of the money judgment).

[41] FED. R. CRIM. P. 32.2(b)(2).

forfeitable property) upon demonstrating that, by the defendant's own act or omission, the directly forfeitable property has been rendered unavailable for criminal forfeiture for any one of five specific reasons.[42] Such substitute assets could potentially include cryptocurrency that is not directly traceable to the criminal offense(s) of conviction. Once any untainted assets of a convicted defendant are located, the government may ask the court to amend the order of forfeiture to include forfeiture of that property.[43]

5. Third parties/ancillary proceedings

After the court issues a preliminary order of forfeiture, whether pursuant to a conviction by a guilty plea or after trial, the government must commence an ancillary proceeding to address any non-defendant, third party interests in the specific property forfeited, which could include third party interests of forfeited cryptocurrency.[44] The government is required to publish notice of the preliminary order and of its "intent to dispose of the property in such manner as the Attorney General . . . direct[s]" and "to the extent practicable, provide direct written notice to any person known to have alleged an interest in the [forfeited] property[.]"[45] The publication of notice should be executed in a manner consistent with the requirements of Supplemental Rule G(4)(a) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (hereinafter Supplemental Rule G). In addition, the government must send direct written notice to any known person who appears to have an interest in the forfeited property, and such notice may be sent by any of the applicable means described in Supplemental Rule G(4)(b)(iii). The notice provides non-defendant third parties the opportunity to file a petition with the court asserting their interests to the forfeited property.

If a third party files a petition asserting an interest in the forfeitable property—whether it be cryptocurrency or some other property—the court must conduct an ancillary proceeding.[46] Upon motion of the government, the court, assuming the facts set forth in the petition are true, may dismiss the petition for lack of standing, for failure to state

[42] *See* 21 U.S.C. § 853(p); 18 U.S.C. § 1963(m).
[43] FED. R. CRIM. P. 32.2(e)(1).
[44] § 853(n)(1); § 1963(l)(1).
[45] § 1963(l)(1); § 853(n)(1).
[46] FED. R. CRIM. P. 32.2(c)(1).

a claim, or for any other legal reason.[47] If the third party claims that he or she is the true owner of an interest in all or part of the property—for example, cryptocurrency—the third party bears the burden of proving either: (1) he or she holds a superior interest to that of the convicted defendant and that interest vested before the government's interest arose upon commission of the crime subjecting the property to forfeiture; or (2) he or she qualifies as a "bona fide purchaser for value" of the property, and had no knowledge, or grounds to know, that the property was subject to forfeiture when purchased or acquired.[48] Prior to holding a hearing on the petition, the court may allow the parties to conduct discovery in accordance with the Federal Rules of Civil Procedure, so long as the court concludes that discovery is necessary or desirable to resolve disputed factual issues.[49] Upon the conclusion of discovery, either party may move for summary judgment pursuant to Federal Rule of Civil Procedure 56. If multiple third party petitions are filed in the same case, an order dismissing or granting one petition cannot be appealed until the court rules on all the petitions, unless the court determines there is no justification for delay.[50]

6. Final order of forfeiture

When the ancillary proceeding has concluded, the court enters a final order of forfeiture by amending the preliminary order, if necessary, to resolve any third party rights to property.[51] In a simple, straightforward case, no third party interests are asserted and the government can submit a proposed final order of forfeiture at or before sentencing.

Generally, seized cryptocurrency is not liquidated until a final order of forfeiture is entered in the criminal case. In the simplest scenario, no third party interests are asserted and a final order of forfeiture is entered at or shortly before sentencing. Any third party claims to the seized cryptocurrency must be adjudicated through the ancillary claims process described above, and any resolved interests should be reflected in the final order of forfeiture. The final order of forfeiture must be made part of the sentence and be included in the Court's

[47] FED. R. CRIM. P. 32.2(c)(1)(A).
[48] *See* § 1963(l)(6); § 853(n)(6).
[49] FED. R. CRIM. P. 32.2(c)(1)(B).
[50] FED. R. CRIM. P. 32.2(c)(3).
[51] FED. R. CRIM. P. 32.2(c)(2).

judgment.[52] At sentencing, the preliminary order of forfeiture becomes final as to the defendant. If the defendant is required to forfeit specific property (such as cryptocurrency) under the order, and third party claims to said property have not been adjudicated in the ancillary proceeding as of sentencing, the forfeiture order will remain preliminary as to third parties until the ancillary proceeding is concluded.[53]

D. Liquidation of forfeited cryptocurrency

Once the forfeitability of seized cryptocurrency is finally adjudicated and a final order of forfeiture has been entered, the Marshals may commence the process of liquidating the seized cryptocurrency through its auction process. The forfeited cryptocurrency from a particular case will likely be pooled with forfeited cryptocurrency from other cases for auction. Auctions are held on a periodic basis, and thus there may be a lag time between the entry of a final order of forfeiture as to specific property that includes cryptocurrency, and the auction of said cryptocurrency.

The Marshals publish a public notice describing the particular type and quantity of cryptocurrency available for sale and inviting parties to submit a bid for purchase pursuant to specified instructions and eligibility requirements. The notice may reference the specific cases in which the subject cryptocurrencies were seized.[54] A recent January 2018 auction of several blocks of Bitcoin, totaling approximately 3,813 bitcoin in all, is estimated to have generated approximately $44 million in revenue.[55]

III. Recent cases involving cryptocurrency

The cases discussed below address common criminal statutes used in charging cases involving cryptocurrencies, and the investigative tools and forfeiture procedures employed in the seizure of cryptocurrency.

---

[52] *See* FED. R. CRIM. P. 32.2(b)(4).

[53] FED. R. CRIM. P. 32.2(b)(4)(A).

[54] An example of an auction notice published online by the U.S. Marshals Service is available at https://www.usmarshals.gov/assets/2018/bitcoinauction/.

[55] Robin La Quercia, *Crypto Auctions: Where Do Arrested Bitcoins End Up*, BITCOINADVICE.COM (Apr. 29, 2018), https://bitcoinadvice.com/crypto-auctions-where-do-arrested-bitcoins-end-up/.

A. *United States v. Ulbricht* (Silk Road Case)

In February 2015, defendant Ross William Ulbricht was convicted after a trial by jury on seven counts arising from his creation and operation of the Silk Road criminal marketplace on the Darknet, under the username Dread Pirate Roberts (DPR). The Silk Road was used primarily to purchase and sell drugs, false identification documents, and computer hacking software, using Bitcoin as the exclusive form of payment. Between 2011 and 2013, approximately $183 million worth of illegal drugs, as well as other goods and services, were sold using the Silk Road. Ulbricht, acting as DPR, earned millions of dollars in illegal profits from the commissions collected by Silk Road on purchases.

In October 2013, the government arrested Ulbricht, seized the Silk Road servers, and shut down the site.[56] Following his conviction at trial, Ulbricht was sentenced to life in prison and ordered to forfeit $183,961,921. Ulbricht appealed his sentence, which was affirmed in all respects by the United States Court of Appeals for the Second Circuit.[57] The United States Supreme Court denied Ulbricht's petition for writ of certiorari.[58]

Prior to trial, Ulbricht moved to dismiss the indictment. In his motion, he argued, among numerous other claims, that, with respect to Count Four of the indictment, "he cannot have engaged in money laundering because all transactions occurred through the use of Bitcoin and thus there was therefore no legally cognizable 'financial transaction.'"[59] The district court rejected Ulbricht's argument. While finding that the fact that "Bitcoins allow for anonymous transactions does not *ipso facto* mean that those transactions relate to unlawful activities," the very fact that "the system of payment [was] designed specifically to shield the proceeds from third party discovery of their unlawful origin . . . forms the unlawful basis of the money laundering charge."[60]

The court further found that the money laundering statute, 18 U.S.C. § 1956,[61] broadly defines "financial transaction" to include

---

[56] United States v. Ulbricht, 858 F.3d 71, 82–83 (2d Cir. 2017).
[57] *See id*.
[58] Ulbricht v. United States, 138 S. Ct. 2708 (2018).
[59] United States v. Ulbricht, 31 F. Supp. 3d 540, 548 (S.D.N.Y. 2014).
[60] *Id*. at 569.
[61] 18 U.S.C. § 1956.

"all movements of 'funds' by any means, or monetary instruments."[62] Because the term, "funds," is not defined in the statute, the court accorded the ordinary definition of funds as "money, often money for a specific purpose"—that is, "money" as an object used to purchase things.[63] Turning to Bitcoin, the court reasoned that "[b]itcoins can be either used directly to pay for certain things or can act as a medium of exchange and can be converted into a currency which can pay for things[.]" As such, the court concluded:

> The money laundering statute is broad enough to encompass use of Bitcoins in financial transactions. . . . Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value. . . . There is no doubt that if a narcotics transaction was paid for in cash, which was later exchanged for gold, and then converted back to cash, that would constitute a money laundering transaction. . . . [Accordingly,] [o]ne can money launder using Bitcoin.[64]

This holding is significant for forfeiture purposes, since there is broad statutory authority to forfeit any property "involved in" money laundering,[65] which the court here held could include the use (and from that, the forfeiture) of Bitcoin to engage in money laundering.

B. *United States v. Faiella*

In *United States v. Faiella*, the defendants were charged in connection with their operation of an underground market for exchanging Bitcoin for fiat currency on the Silk Road website. Defendant Faiella was specifically charged with operating an unlicensed money transmitting business in violation of 18 U.S.C. § 1960, and conspiring to commit money laundering in violation of 18 U.S.C. § 1956(h). After indictment, Faiella moved to dismiss the section 1960 charge, arguing that Bitcoin does not qualify as "money" under the statute, that operating a Bitcoin exchange does

[62] *Ulbricht*, 31 F. Supp. 3d at 570.
[63] *Id.*
[64] *Id.*
[65] *See* 18 U.S.C. §§ 981(a)(1)(A) (civil forfeiture), 982(a)(1) (criminal forfeiture).

not constitute "transmitting" money under the statute, and that he did not qualify as a "money transmitter" under the statute.[66]

Relying on plain meaning definitions, the court first determined that "Bitcoin clearly qualifies as 'money' or 'funds'" that "can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions."[67] Second, the court concluded that "Faiella's activities on Silk Road constitute[d] 'transmitting' money under Section 1960[,]" given the allegation that "Faiella received cash deposits from his customers and then, after exchanging them for Bitcoins, transferred those funds to the customers' accounts on Silk Road."[68] Therefore, "in sending his customers' funds to Silk Road, Faiella 'transferred' them to others for a profit."[69] Third, the court held that "Faiella clearly qualifie[d] as a 'money transmitter' for purposes of Section 1960," based on guidance issued by the Financial Crimes Enforcement Network (FinCEN), "specifically clarifying that virtual currency exchangers constitute 'money transmitters' under its regulations."[70] Finally, the court rejected defendant's claim that applying section 1960 to a Bitcoin exchange business would violate the rule of lenity, "constituting such a novel and unanticipated construction of the statute as to operate an *ex post facto* law in violation of the Due Process Clause."[71] The court found that there was "no . . . irreconcilable ambiguity" in the statute's language and structure, legislative history, and motivating policies that would require resort to the rule of lenity.[72]

This case is notable in the forfeiture context, as there is wide statutory authority to forfeit any property "involved in" an 18 U.S.C. § 1960 offense, or any property traceable to such property, which, in this context, could include the Bitcoin exchanged in the illegal money transmitting business.[73]

C. *United States v. 50.44 Bitcoins*

In December 2015, the United States filed a verified complaint for forfeiture against 50.44 bitcoins. The Clerk filed an entry of default on

---

[66] United States v. Faiella, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014).
[67] *Id.*
[68] *Id.* at 546.
[69] *Id.*
[70] *Id.*
[71] *Id.* at 547.
[72] *Id.*
[73] *See* 18 U.S.C. §§ 981 (civil forfeiture), 982 (criminal forfeiture).

March 9, 2016, and the United States filed a motion for default judgment on March 10, 2016. No response to the motion was filed. The matter was referred to a magistrate judge for report and recommendations, and the magistrate recommended that the motion for default judgment be granted. In reaching this conclusion, the court assessed whether the government had established that there was a substantial connection between the property—that is, the Bitcoin—and the offense, under 18 U.S.C. § 983(c)(3). The court found that because the business operated by Amanda and Thomas Callahan under the Silk Road username, "JumboMoneyBiscuit," was not registered to transmit money as required by state and federal law, the Callahans violated section 1960. Accordingly, the 50.44 Bitcoins seized from the Callahans constituted property "involved in" a transaction that violated section 1960. Moreover, "[b]ecause the United States ha[d] established a substantial connection between the property to be forfeited and a criminal offense, the 50.44 Bitcoins [we]re subject to forfeiture under 18 U.S.C. § 981 and 983."[74]

The court further found that that the government had complied with Supplemental Rule G's procedural requirements governing the pleading of the civil forfeiture complaint and its notice requirements. Accordingly, "[b]ecause the United States ha[d] complied with the procedural requirements of Rule G and ha[d] met the substantive requirements of 18 U.S.C. § 981, [the court found] that the 50.44 Bitcoins seized from the Callahans [we]re subject to forfeiture."[75]

In June 2016, the district court entered an order agreeing with the magistrate judge's report and recommendation in every respect, entering judgment in favor of the United States against the 50.44 Bitcoins, forfeiting the property to the United States pursuant to 18 U.S.C. § 981(a)(1)(A), and authorizing the Attorney General, or a designee, to seize the forfeited property and take exclusive custody and control of it until its disposal in accordance with the law.[76]

D. *United States v. Vallerius*

In this case, defendant Gal Vallerius moved to suppress certain statements and physical evidence. Vallerius had been arrested for his

[74] United States v. 50.44 Bitcoins, No. CV ELH-15-3692, 2016 WL 3049166, at *2 (D. Md. May 31, 2016).
[75] *Id*. at *3.
[76] *See* Order, United States v. 50.44 Bitcoins (Callahan), No. ELH-15-3692 (D. Md. June 20, 2016).

use of the Darkweb to facilitate international narcotics transactions. Specifically, Vallerius had used the "Dream Market," a website on the Darknet that allowed individuals to create online advertisements offering various narcotics for sale at a set price. Payment for the illicit purchases were made through Bitcoin and other cryptocurrencies, "which add[ed] an additional layer of anonymity to the transaction and conceal[ed] the identities of the accounts from which the cryptocurrency payments originate[d]."[77] Vallerius, as a "senior moderator" on the Dream Market website and using the moniker "OxyMonster," moderated the forums and provided advice to other members about the online drug trade. Vallerius also sold controlled substances to other members using the website, receiving payment for the sales through the use of a Bitcoin "tip jar," or electronic depository. It was through this "tip jar" that law enforcement officials became aware of Vallerius' true identity. Agents tracked several incoming payments and outgoing deposits from the tip jar to various wallets controlled by Vallerius. Agents also compared posts made by OxyMonster on the Dream Market forum with social media accounts used by Vallerius, and determined that the writing style and syntax of OxyMonster's posts on Dream Market matched those written by Vallerius on his social media accounts.[78]

Law enforcement learned that Vallerius would be travelling to the United States from Paris, France, and making entry on August 31, 2017. Upon his arrival at the Atlanta, Georgia airport, Vallerius was "flagged" and pulled aside for secondary inspection by United States Customs and Border Protection (CBP) officers. CBP officers asked Vallerius to open his bags and asked if he was traveling with any electronic devices. He acknowledged that he possessed a laptop computer, a cell phone, and an iPad tablet. The agent asked if the devices were password protected and Vallerius replied in the affirmative. The agent informed him that he would have to provide the passwords to the electronics because the devices were subject to routine inspection at the border. Vallerius complied, providing his passwords, and the electronic devices were removed from his possession. The computer, tablet, and cell phone were transferred to

[77] United States v. Vallerius, No. 17-CR-20648, 2018 WL 2325729 (S.D. Fla. May 1, 2018), report and recommendation adopted, No. 17-20648-CR, 2018 WL 2324059 (S.D. Fla. May 22, 2018).
[78] *Id*. at *1.

the custody of DEA agents, who used the passwords to gain access to the computer and conduct a search of its contents.

On the laptop, the agents located a Bitcoin wallet that they believed could be traced to the OxyMonster account. The agents had the CBP officer request the wallet password from Vallerius, who in response claimed that no password was required for the wallet. Vallerius was then placed under arrest and advised of his *Miranda* rights. Agents then attempted to question him about the contents of the laptop. Vallerius indicated that he wished to consult with an attorney, and the agents thereupon stopped the interview. A search warrant was subsequently obtained to conduct a complete examination of Vallerius' computer.[79]

Vallerius moved to suppress, claiming that initial questioning by the CBP officer, during which the officer requested the computer password and the cell phone personal identification number (PIN) code violated the Fifth Amendment, and that any information obtained as a result of that conversation should be suppressed. In addressing Vallerius's motion, the court first considered whether asking the defendant to provide his computer password and cell phone PIN code, without first *Mirandizing* him, violated the Fifth Amendment. The court observed that, "in the case of those seeking entry to the United States, whether such a person can be considered 'in custody' for purposes of *Miranda* 'should be interpreted in light of the strong government interest in controlling [our nation's] borders.'"[80]

Applying factors set forth by the Eleventh Circuit in *United States v. Moya*,[81] the court concluded that "Vallerius was not in custody at the time he provided his password and PIN codes." He was not placed in handcuffs, no guns were drawn on him when he provided the information, and he never asked to leave the secondary inspection area.[82] The court further found that the border search did not "taint" the subsequent search warrant obtained for the computer.[83] The magistrate recommended that the defendant's motion to suppress be

[79] *Id*. at *2–3.
[80] *Id*. at *3.
[81] United States v. Moya, 74 F.3d 1117 (11th Cir. 1996).
[82] *Vallerius,* 2018 WL 2325729, at *4.
[83] *Id*. at *7.

denied, and the district court adopted the report and recommendation by order filed on May 22, 2018.[84]

This decision is notable, as it may provide authority for asking a subject for not only passwords to access a computer or smart phone, on which evidence of cryptocurrency may be stored, but also for asking for the private key for a cryptocurrency wallet stored therein, at least in the context of a border search.

E. *United States v. 2013 Lamborghini Aventador LP700-4* (AlphaBay Case)

In this in rem civil forfeiture action, the United States filed an ex parte motion for default judgment and final judgment of forfeiture as to several luxury vehicles, bank accounts, real properties, and millions of dollars in various cryptocurrencies. In July 2017, the United States filed a verified first amended forfeiture complaint alleging that between December 2014 and July 2017, the AlphaBay website on the Darknet served as a marketplace for illegal goods such as malware, controlled substances, chemicals, guns, stolen financial information, and counterfeit documents to its users all over the world, including in the Eastern District of California. An individual named Alexandre Cazes founded AlphaBay in 2014 and was its leader through July 4, 2017. He oversaw Alphabay's operations and controlled the profits generated from the operation of the business, receiving tens of millions of dollars in commissions from the illegal transactions facilitated by Alphabay. Alphabay required its users to transact in cryptocurrencies such as Bitcoin, Monero, and Ethereum.[85]

During the investigation stage of the case, between May 2016 and June 2017, United States law enforcement agents made numerous undercover purchases of marijuana, heroin, fentanyl, and methamphetamine; fake identification documents; and an ATM skimmer from AlphaBay vendors. During the course of their investigation, they identified Cazes as "Alpha02" and "Admin," the founder and administrator of AlphaBay. They learned that the personal email address, "Pimp_Alex_91@hotmail.com," was included in the header of AlphaBay's "welcome email" to new users, and in the

---

[84] *See* Order Adopting Magistrate Judge's Report and Recommendation, United States v. Vallerius, Crim. No. 17-20648-CR-Scola, 2018 WL 2324059 (S.D. Fla. May 22, 2018).

[85] United States v. 2013 Lamborghini Aventador LP700-4, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018).

header of AlphaBay's "password recovery process" for users who lost their passwords to the AlphaBay forum. Law enforcement then learned that the email address belonged to Cazes, a Canadian national.[86]

When law enforcement executed a search warrant at Cazes' residence, he was in active communication with one of the AlphaBay data centers about a law enforcement-generated service outage on the site. In addition, passwords to AlphaBay's servers and other evidence was found on Cazes' personal computer linking him to the website. Law enforcement also determined that Cazes owned and controlled a front company called EBX Technologies, which he used to "justify his banking activity and substantial cryptocurrency holdings."[87]

In June 2017, a warrant was issued for Cazes' arrest based upon a 16-count indictment[88] charging him with, among other things, RICO conspiracy, drug conspiracy, conspiracy to commit identify theft and access device fraud, and conspiracy to commit money laundering. The indictment also sought to forfeit all assets connected to the AlphaBay criminal organization. Additionally, in June 2017, a federal judge in the United States found probable cause to issue seizure warrants for a luxury vehicle and eleven bank and cryptocurrency exchange accounts traceable to unlawful proceeds generated from AlphaBay. Law enforcement had traced Bitcoin transactions conducted in AlphaBay to digital currency accounts, bank accounts, and other assets owned by Cazes and his wife.[89] In Thailand, where Cazes lived with his wife, law enforcement also identified numerous bank and digital exchange accounts tied to Cazes containing illicit proceeds from AlphaBay operations, which digital exchange accounts Cazes used to liquidate his cryptocurrency (usually Bitcoin) so that he could spend the proceeds in Thailand and other countries on expensive cars, real estate holdings, and other assets.[90]

---

[86] *Id.* at *4.

[87] *Id.* at *4–5.

[88] *Id.* at *4 (dismissing all 16 counts of the indictment in April 2018, following Cazes' death; the civil forfeiture action survived, as the government may still seek civil forfeiture of the property of defendants who have died). *See* United States v. Real Property at 40 Clark Road, 52 F. Supp. 2d 254, 265 (D. Mass. 1999) (explaining that defendant's death during the pendency of the criminal forfeiture proceedings made civil forfeiture necessary).

[89] *Lamborghini*, 2018 WL 3752131 at *5.

[90] *Id.*

On July 5, 2017, the Royal Thai Police, with assistance from the FBI and the DEA, executed an arrest warrant for Cazes, as well as a search warrant at his primary residence in Bangkok, Thailand. At the time of his arrest, his laptop was open and in an unencrypted state, and logged into the AlphaBay forums and the server that hosted the AlphaBay website under the username, "Admin." Because his computer was unlocked and unencrypted, law enforcement was able to search Cazes' computer and found several open text files with passwords/passkeys for the AlphaBay website, all of the AlphaBay servers, and other online identities associated with AlphaBay. As a result, law enforcement was able to seize all of the information and cryptocurrency on the AlphaBay servers. Additionally, law enforcement found a document containing wallet addresses with the private keys written next them, which allowed law enforcement to transfer the cryptocurrency in each wallet to a secure government-controlled wallet address. In total, from Cazes' wallets and computer, agents assumed control of approximately $8,800,000 in Bitcoin, Ethereum, Moreno, and Zcash. Law enforcement also identified and seized certain servers that hosted AlphaBay cryptocurrency wallets, some unencrypted and others encrypted. In addition, law enforcement seized information and cryptocurrency from IP addresses containing AlphaBay's entire universe of cryptocurrency.[91]

The United States filed its civil forfeiture complaint on July 19, 2017, and an amended forfeiture complaint on July 26, 2017. Based on the allegations in the amended complaint, the Clerk of Court issued a warrant for arrest of articles in rem for the defendant assets. In August 2017, the court issued an order allowing public notice of the forfeiture action for 30 consecutive days on the official government forfeiture website, www.forfeiture.gov. Publication began on September 27, 2017, and ran for at least 30 consecutive days, consistent with Supplemental Rule G(4)(a). The United States also provided notice to various potential claimants who might have had an interest in the defendant properties. In addition, the government coordinated with the governments of Thailand, Antigua, and Cyprus to post copies of the notice of the forfeiture complaint on the real properties purchased by Cazes in those countries. On November 14, 2017, the Clerk of Court entered default against all of the known

[91] *Id*. at *5–7.

claimants, and the United States filed an ex parte motion for default judgment and final judgment of forfeiture on June 1, 2018.[92]

In determining whether the government's motion for default judgment should be granted, the court first determined the sufficiency of the forfeiture complaint. With respect to the cryptocurrency, specifically, the court observed that the complaint alleged that "[f]ederal agents traced Bitcoin transactions originating with AlphaBay to digital currency accounts, and ultimately bank accounts and other tangible assets held by Cazes and his wife." The complaint further alleged that "Cazes concealed and disguised the illicit source of the funds by commingling the criminal proceeds in digital currency exchange accounts and bank accounts controlled by Cazes and his wife, and using an automated mixing and tumbling procedure designed to conceal the source of the criminal funds when converting Bitcoin (and other cryptocurrencies) to currency." The complaint also alleged that at the time of his arrest, Cazes' laptop was logged into the server hosting the AlphaBay website and law enforcement identified passwords and passkeys for, among other things, the cryptocurrency wallets contained on each server. Law enforcement also, the complaint alleged, found a document listing, among other things, Cazes' cryptocurrency holdings. Given the absence of asserted interests in the defendant assets, the court "therefore [found] that the facts, as alleged, provide[d] a sufficient connection between the Defendant Assets and illegal money laundering, racketeering, fraud, and drug activity, to support forfeiture."[93]

The court also found that the government had satisfied Supplemental Rule G's notice requirements, as to the defendant properties, that the time to file a claim had expired, and that therefore the Clerk of Court properly had entered defaults against the potential claimants. The magistrate concluded, therefore, that the government had met the procedural requirements for civil in rem forfeiture actions set forth in 18 U.S.C. §§ 983 and 985, and recommended the granting of the government's ex parte motion for default judgment, and the entry of a final judgment of forfeiture to be submitted by the government.[94] The district court's decision as to whether to adopt the findings and recommendations of the magistrate court are still pending as of the writing of this article.

---

[92] *Id*. at *9.

[93] *Id*. at *11–12.

[94] *Id*. at *14.

This case exemplifies the tremendous success that can be achieved through careful pre-seizure investigation and planning, utilizing investigative techniques aimed to identify "dirty" cryptocurrency transactions and Darknet activity, and tracing those transactions to a specific individual.

IV. Conclusion

As demonstrated above, asset forfeiture plays a critical role in the identification, seizure, preservation, and liquidation of cryptocurrency that is used to engage in criminal activity. Asset forfeiture allows law enforcement to take "tainted" cryptocurrency out of the hands of wrongdoers who exploit the anonymity of cryptocurrency to operate and profit from criminal enterprises.

About the Author

Shirley U. Emehelu is Chief of the Asset Recovery and Money Laundering Unit (ARMLU) at the United States Attorney's Office for the District of New Jersey (DNJ), where she has been an Assistant United States Attorney in the Newark office since 2010. As Chief of ARMLU, Ms. Emehelu supervises the unit's Asset Forfeiture, Money Laundering, and Financial Litigation Assistant United States Attorneys and support staff. Prior to becoming Chief of ARMLU, Ms. Emehelu was an Assistant United States Attorney in DNJ's Economic Crimes Unit. Following her tenure in the Economic Crimes Unit, Ms. Emehelu was in the Special Prosecutions Division of the United States Attorney's Office, where she investigated and prosecuted public corruption cases, many of which involved financial fraud.

Prior to joining the United States Attorney's Office, Ms. Emehelu worked as a litigation associate in the New York office of a global law firm, where her practice focused on internal corporate investigations, federal grand jury and regulatory investigations, corporate compliance, and complex commercial litigation.

Additionally, Ms. Emehelu served as an Adjunct Professor at Montclair State University in the fall of 2014, where she taught White Collar Crime in the University's Justice Studies department. Ms. Emehelu clerked for the Honorable James R. Spencer in the Eastern District of Virginia. She received her J.D. from Yale Law School, where she was an Editor for the Yale Law Journal and a Member of the Journal's Admissions Committee, and her bachelor's degree in Political Science, with distinction, from Yale University.

Page Intentionally Left Blank

18 U.S.C. § 1348—A Workhorse Statute for Prosecutors

Sandra Moser
Acting Chief, Fraud Section
Criminal Division
United States Department of Justice

Justin Weitz
Assistant Chief, Fraud Section's Securities & Financial Fraud Unit
Criminal Division
United States Department of Justice

I. Introduction

In the wake of the dramatic corporate scandals of the early 2000s—the collapse of Enron and the failures at WorldCom and Tyco, among others—Congress enacted a package of new laws designed to tighten accounting protocols, improve compliance procedures, and deter criminal fraud at public companies.[1] The Sarbanes-Oxley Act of 2002 mandated a number of reforms, and also added new provisions to the federal criminal code, in order to "provide needed enforcement flexibility and, in the context of publicly traded companies, protection against all the types of schemes and frauds which inventive criminals may devise in the future."[2] One such provision, 18 U.S.C. § 1348, penalizes securities fraud (and, as a result of a later amendment, commodities fraud) and can serve as an advantageous statute for prosecutors seeking to charge complex white collar cases.

In the 16 years since the enactment of section 1348, courts have read the statute broadly, often comparing it to the textually similar bank fraud statute, 18 U.S.C. § 1344. Such broad readings are helpful for the Department, as they give prosecutors the ability to target

[1] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 807(a), 116 Stat. 745, 804 (2002), *amended by* Pub. L. No. 111-21, § 2(e)(1), 123 Stat. 1617, 1618 (2009). The 2002 law, commonly referred to as "Sarbanes-Oxley" after its principal Congressional sponsors, was formally titled the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House).

[2] COMM. ON THE JUD., THE CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY ACT OF 2002, 107TH CONG., S. Rep. No. 107–146, at 20 (2002).

fraudulent and deceptive conduct that may not fit within the confines of the familiar wire and mail fraud statutes. Section 1348, particularly its first subsection, is thus a promising development for white collar prosecutors, who can utilize it to charge certain types of schemes without the limitations placed on the use of the mail fraud, wire fraud, and traditional securities fraud statutes.

This article explores judicial interpretations of section 1348(1), and how prosecutors can use the statute to reach securities and commodities fraud schemes in which there is no evidence of direct misrepresentations or material omissions with a duty to disclose. This article further discusses other advantages of using section 1348(1) to reach schemes affecting securities and commodities markets. Finally, this article raises several practice pointers for prosecutors seeking to charge cases under section 1348(1).

II. Securities and commodities fraud under section 1348(1) generally

Title 18, United States Code, section 1348, states in relevant part:

> 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. 78l) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(d));
>
> . . .
>
> shall be fined under this title, or imprisoned not more than 25 years, or both.[3]

[3] *Compare* 18 U.S.C. § 1348(1), *with* § 1348(2) which makes it a crime "to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale" of covered securities and commodities. Section 1348(2)'s focus on "false or fraudulent pretenses, representations, or promises" suggests it is best read as an analogue of the mail and wire fraud statutes, or 18 U.S.C. § 1344(2), and requires material misrepresentations in order to be properly charged. This article focuses solely on section 1348(1).

Congress passed section 1348 with full knowledge that securities fraud was already a criminal offense prior to 2002, as codified in Title 15 and accompanying SEC regulations such as Rule 10b-5, which was promulgated pursuant to the Securities Exchange Act of 1934.[4] Congress added section 1348 to the chapter of Title 18 which addresses schemes to defraud more generally, placing it alongside the statutes which criminalize mail and wire fraud, bank fraud, and health care fraud. Section 1348 was thus created to streamline and broaden securities fraud prosecutions, which Congress feared were unnecessarily complicated by regulations and technical requirements, and "to provide a flexible tool to allow prosecutors to address the wide array of potential fraud and misconduct which can occur in companies that are publicly traded."[5] Despite the broad and aggressive approach that Congress sought in enacting and later expanding the statute, many securities fraud prosecutions still proceed under 10b-5.

In 2009, Congress further broadened section 1348 by expanding it to cover schemes to defraud that involved commodities futures and options contracts related to commodities futures. This expansion has brought within its ambit a new range of conduct that does not fall within the familiar and well-trod ground of 10b-5.

In recent years, prosecutors have brought a host of unique cases under section 1348. These include traditional securities fraud cases involving material misrepresentations in filings, accounting fraud, insider trading, and other conduct that might previously have been handled pursuant to 10b-5 or the mail and wire fraud statutes. Prosecutors, however, are also using section 1348 to pursue less common conduct, such as schemes to defraud by broker-dealers, spoofing in commodities futures markets, and market manipulation.

III. Similarities to bank fraud under section 1344(1)

Section 1348 was designed as an analogue to 18 U.S.C. § 1344, the bank fraud statute, and was intended to broaden the scope of securities fraud prosecutions. Section 1348 was created with

---

[4] *See generally* 15 U.S.C. §§ 78j(b), 78ff; 17 C.F.R. § 240.10b-5.

[5] *See*, *e.g.*, 148 CONG. REC. S7418-01 (daily ed. July 26, 2002) (statement of Sen. Leahy) (noting that section 1348 "would supplement the patchwork of existing technical securities law violations with a more general and less technical provision . . .").

"elements and intent requirements comparable to . . . bank fraud and health care fraud statutes."[6] Section 1344, therefore, should guide courts on how to interpret section 1348(1).

The bank fraud statute offers the government two avenues to a conviction. Subsection (1), which mirrors section 1348(1), penalizes a "scheme to defraud a financial institution." Subsection (2), which mirrors section 1348(2), focuses on attempts to obtain money by way of false representations. Recently, the Supreme Court held in *Loughrin v. United States* that the bank fraud statute is to be read disjunctively, with each prong criminalizing a distinct type of conduct.[7]

More significantly, the *Loughrin* Court also noted that section 1344(1) did not require the use of false statements in order to execute a scheme to defraud, and was thus distinguishable from the mail and wire fraud statutes.[8] This echoed the pre-*Loughrin* consensus among the circuits that "a person may commit a bank fraud without making false or fraudulent pretenses, representations or promises, as this is the 'plain meaning' of the statute."[9] Unlike the

---

[6] *Id.*

[7] *See* Loughrin v. United States, 134 S. Ct. 2384, 2389–90 (2014). The Supreme Court addressed the bank fraud statute again two years later in *Shaw v. United States*, though its primary focus in *Shaw* was on section 1344(2). Shaw v. United States, 137 S. Ct. 462 (2016).

[8] *Loughrin*, 134 S. Ct. at 2390–91 & n.4 (noting that 18 U.S.C. § 1344 has two separate prongs and thus constitutes two distinct crimes, unlike the mail and wire fraud statutes which are traditionally viewed as a single crime (citing McNally v. United States, 483 U.S. 350, 358–59 (1987))).

[9] United States v. Schwartz, 899 F.2d 243, 246 (3d Cir. 1990); *see, e.g.*, United States v. Steffen, 687 F.3d 1104, 1112 & n.5 (8th Cir. 2012) (collecting cases) ("[S]ection 1344(1) does not require an affirmative misrepresentation"); United States v. LeDonne, 21 F.3d 1418, 1425 (7th Cir. 1994) ("In applying the disjunctive analysis to bank fraud, courts have required proof of a misrepresentation only to convict for a violation of [Section] 1344(2)."); United States v. Ragosta, 970 F.2d 1085, 1089 (2d Cir. 1992) ("[Section] 1344(1) does not require proof of a misrepresentation."); United States v. Stone, 954 F.2d 1187, 1190 (6th Cir. 1992) (following the "number of courts" that "have not required an affirmative misstatement to support a conviction" under Section 1344(1)); United States v. Fontana, 948 F.2d 796, 800 (1st Cir. 1991) (Section 1344 does not require an additional showing of misrepresentation); United States v. Celesia, 945 F.2d 756, 758 (4th Cir. 1991) ("[O]ne may commit a bank fraud under Section 1344(1) by defrauding a financial institution, without making the false or fraudulent

mail and wire fraud statutes, which generally require false and material representations, pretenses, or promises in order to sustain a conviction, the bank fraud statute does not; instead, it is generally understood to require fraudulent intent and deceptive conduct in pursuit of a scheme to defraud a financial institution.

IV. Specific applications of section 1348(1)

Since section 1348 is framed in language almost identical to section 1344, proper analysis of section 1348(1) should follow a similar logic, and convictions under section 1348(1) should not require false or fraudulent representations, pretenses, or promises. Although defendants in section 1348(1) cases have at times attempted to impose this additional requirement upon the government, two Courts of Appeal, as of this writing, have endorsed the proposition that a conviction under section 1348(1) does not require affirmative misrepresentations or material omissions.

In 2012, the Second Circuit was the first to weigh in. In *United States v. Mahaffy*, the court stated that "[f]alse representations or material omissions are not required for a conviction under § 1348(1)."[10] The *Mahaffy* panel explained that the elements of a conviction under section 1348(1) are "(1) fraudulent intent, (2) [a] scheme or artifice to defraud, and (3) nexus with a security." Accordingly, the *Mahaffy* panel found that "the jury could have convicted under [section] 1348 without considering false representations or material omissions."[11]

In 2017, the Seventh Circuit adopted the same view in *United States v. Coscia*, quoting *Mahaffy* and noting that the three elements of a conviction under section 1348(1) are "(1) fraudulent intent, (2) a scheme or artifice to defraud, and (3) a nexus with a

---

promises required by Section 1344(2)."); United States v. Cronic, 900 F.2d 1511, 1513–14 (10th Cir. 1990) ("The offense of a scheme to defraud focuses on the intended end result, not on whether a false representation was necessary to effect the result. Schemes to defraud, therefore, may come within the scope of [Section 1344] even absent an affirmative misrepresentation.").

[10] United States v. Mahaffy, 693 F.3d 113, 125 (2d Cir. 2012).

[11] *Id.* The *Mahaffy* panel did not need to reach the issue since it also found that the government had established that the defendants omitted material facts despite a duty to disclose, but nonetheless chose to address and articulate the standard for section 1348(1) convictions.

security [or commodity]."[12] The Seventh Circuit also rejected Coscia's argument that the deceptive conduct itself needed to be "material," which would have indirectly added a material misrepresentation element to section 1348(1).

Mahaffy and *Coscia* provide legal and factual guidance to white collar prosecutors. Both appellate courts unequivocally stated that none of the usual hallmarks of wire and mail fraud—false statements, representations, and promises, or material omissions made with a duty to disclose—must be present in a section 1348(1) indictment. Rather, a pattern of deceptive conduct can be enough for the government to sustain its burden in a section 1348 prosecution. As to what facts constitute a legally supportable charge, the specific facts of these cases may assist prosecutors in determining what types of deceptive conduct fall under the rubric of section 1348(1), and help prosecutors to find an appropriate charge for cases that do not fit the traditional mail and wire fraud model.

First, *Mahaffy* involved brokers at one firm who received kickbacks for providing confidential information to another day trading firm. The case did not fit neatly into the familiar insider trading or mail and wire fraud model, but was chargeable under section 1348(1). Indeed, in reviewing the charges brought under section 1348(1), the district court in *Mahaffy* articulated a broad approach, which should permit prosecutors to proceed in cases where material omissions were made, but where the relationship between the defendant and the victim is insufficient to support a wire or mail fraud theory. Noting that the statute reached schemes to defraud "any person," the district court stated that section 1348(1) "does not restrict, or even contemplate, the status of the victim."[13] Whereas, mail and wire fraud cases operating on omissions theories traditionally require the government to show that the defendants violated a duty to disclose information to the victim, *Mahaffy* suggests that this principle does not apply in section 1348(1) prosecutions. Pointing out that Congress modeled section 1348 off the bank and health care fraud statutes, the district court stated that the intent of section 1348(1) was "to prohibit all forms of fraudulent conduct associated with securities. . . ."[14] This

[12] United States v. Coscia, 866 F.3d 782, 796 (7th Cir. 2017), *cert. denied,* Coscia v. United States, 138 S. Ct. 1989 (2018).
[13] United States v. Mahaffy, No. 05-CR-613, 2006 WL 2224518, at *12 (E.D.N.Y. Aug. 2, 2006).
[14] *Id.*

broad statement of purpose offers prosecutors an avenue to pursue cases that might fail in other contexts for lack of a cognizable legal duty.

In *Coscia*, the indictment alleged that the defendant had operated a computer program which "spoofed" commodities futures markets by placing large orders in an attempt to trick other market participants into believing there was artificial supply or demand.[15] In reviewing the defendant's conviction on appeal, the Seventh Circuit noted that Coscia had "designed a scheme to pump and deflate the market through the placement of large orders" and that "[h]is scheme was deceitful because, at the time he placed the large orders, he intended to cancel the orders."[16] This deceit without more, according to the court, was sufficient to sustain a conviction under section 1348(1).

In fact, the district court below in *Coscia* took care to note that the indictment specifically alleged deceptive conduct in the absence of false representations. In its opinion denying the defendant's motion to dismiss the indictment, the district court directly quoted from the indictment, which alleged Coscia had "carried out his strategy to 'create a false impression regarding the number of contracts available in the market, and to fraudulently induce other market participants to react to the deceptive market information' . . ."[17] The district court further noted that the indictment alleged Coscia "intended to trick others into reacting to the false price volume information he created with his fraudulent and misleading quote orders . . . [sic] [and] intended to, and did, mislead other traders, causing them to react, [sic]"[18] Even without false statements or representations, Coscia's fraudulent intent provided a sufficient basis to allege a criminal violation, the trial court concluded.

Coscia thus blessed the use of section 1348(1) in market manipulation and spoofing cases where the charged conduct was alleged to be undertaken with the intent to defraud. Indeed, this approach was echoed recently in the District of Connecticut in *United States v. Flotron*. In *Flotron*, the defendant was charged with conspiracy to commit commodities fraud pursuant to 18 U.S.C. § 1349, as a result of his "spoofing" in the precious metals futures markets. In

---

[15] 7 U.S.C. § 6c(a)(5)(C) (defining "spoofing" as "bidding or offering with the intent to cancel the bid or offer before execution").

[16] *Coscia*, 866 F.3d at 797.

[17] United States v. Coscia, 100 F. Supp. 3d 653, 660 (N.D. Ill. 2015).

[18] *Id.*

a pretrial ruling denying the defendant's motion to dismiss, the *Flotron* court, citing *Mahaffy*, recognized that "a scheme to defraud does not necessarily require the prosecution to prove that there were any false statements or explicit misrepresentations."[19] Explicitly stating that the bank fraud statute "is highly similar to the commodities fraud statute at issue here," the *Flotron* court deemed it sufficient "if a defendant while acting with intent to defraud knowingly engages in conduct—as distinct from explicit misrepresentations—to deceive someone else."[20]

The *Flotron* court further noted that conduct knowingly undertaken with the intent to defraud could be broadly defined. Stating that "[f]raudulent schemes often involve acts that seem innocuously innocent when viewed in isolation but that are part-and-parcel of a scheme to defraud when viewed in their broader context."[21] The *Flotron* court cited *United States v. Finnerty* for the proposition that "[c]onduct itself can be deceptive[.]"[22] The trial judge's jury instructions echoed his pretrial ruling, stating that a "'scheme to defraud' . . . need not necessarily involve any false statement or misrepresentation of fact if it otherwise involves deceptive conduct."[23]

The jury instructions given in *Coscia* and *Flotron* offer valuable guidance for charging market manipulation in securities and commodities fraud cases without having to point to specific misrepresentations or reliance on those representations.[24] The *Flotron*

---

[19] United States v. Flotron, No. 3:17-CR-00220 (JAM), 2018 WL 1401986, at *2 (D. Conn. Mar. 20, 2018).

[20] *Id.* at *2 & n.2.

[21] *Id.* at *3.

[22] *Id.* at *2. (citing United States v. Finnerty, 533 F.3d 143, 150 (2d Cir. 2008)). *Finnerty* is a cautionary tale for prosecutors, however. The Second Circuit reversed Finnerty's conviction because his conduct—using his position as a stockbroker to interposition and profit off clients' trades—lacked any deceptive character. Section 1348 offers prosecutors an opportunity to broaden the scope of chargeable conduct, but it of course does not automatically convert every regulatory violation into a criminal scheme.

[23] *See* Trial Transcript at 1311–12, United States v. Flotron, No. 3:17-CR-00220 (D. Conn. 2017).

[24] Title 15 contains a provision criminalizing securities price manipulation. 15 U.S.C. § 78i. Title 7 contains an analogous provision criminalizing market manipulation in the commodities markets. 7 U.S.C. § 9. In *Coscia*, the Seventh Circuit suggested that section 1348 could offer a broader theory of

instruction included the helpful language that the government need not prove "that another market participant was actually deceived . . . so long as there is proof that the scheme to defraud was at least capable of affecting that participant's conduct or decision in the market in a manner that could lead either to some gain for the wrongdoer or some harm to the victim."[25] This materiality instruction suggests that market participants, who often are sophisticated themselves, need not be deceived for a defendant to have committed a violation of section 1348. This possibility offers prosecutors ammunition in arguing that the deceptive conduct charged in securities fraud cases is sufficient even in the absence of unsophisticated counterparties or sympathetic victims.[26]

Other district courts generally have embraced this approach, finding that section 1348(1) does not require proof of material misrepresentations.[27] For example, in *United States v. Melvin*, a district court in the Northern District of Georgia rejected a challenge to section 1348(1)'s use in an insider trading prosecution.[28] The court, citing the three familiar elements of section 1348 articulated elsewhere, further noted that section 1348 did not incorporate the provisions of 10b-5 insider trading, giving prosecutors additional flexibility to use in insider trading cases.

Prosecutors should, however, exercise caution when proceeding under section 1348(1), and ensure that judges do not instruct juries in a way that conflates the two subsections of section 1348. As of this writing, no circuit has yet published a pattern jury instruction for violations of section 1348. Prosecutors should be vigilant in keeping the court informed of the critical difference between the requirements

---

liability for price manipulation than those statutes in Title 15 and 7. *See* United States v. Coscia, 866 F.3d 782, 797 n.64 (7th Cir. 2017).

[25] *Flotron*, Trial Tr. at 1312.

[26] *See generally* United States v. Litvak, 889 F.3d 56 (2d Cir. 2018) (reversing the conviction of a broker based on the materiality of statements he made to counterparties about broker profits). *Litvak* was brought under 10b-5. Had the case been brought under section 1348, the mere existence of deceptive conduct could have shifted the discussion away from the materiality of the defendant's statements and towards the overall scheme to defraud.

[27] *See*, *e.g.*, United States v. Wey, No. 15-CR-611 (AJN), 2017 WL 237651, at *9–10 (S.D.N.Y. Jan. 18, 2017); Donaldson v. Severn Sav. Bank, F.S.B., No. JKB-15-901, 2015 WL 7294362, at *5 n.1 (D. Md. Nov. 18, 2015) (citing United States v. Mahaffy, 693 F.3d 113, 125 (2d Cir. 2012)).

[28] United States v. Melvin, 143 F. Supp. 3d 1354, 1372 (N.D. Ga. 2015).

of the wire and mail fraud statutes, and the elements of section 1348(1), lest other courts omit the differences between the two statutes and impose additional elements that the government may be unable, and is not required, to prove. In cases where the government is proceeding under both prongs of section 1348, the government should consider seeking separate instructions and a special verdict form for both subsections; when the government is proceeding only under section 1348(1), it should ensure that the district court does not insert a "false statements" element into the jury charge.

In addition, the district court rulings in *Coscia* and *Flotron* can assist prosecutors in drafting charges under section 1348(1). The statute does not require proof of false statements, but prosecutors would be wise to allege specific examples of deceptive conduct in the indictment where possible; both district courts in *Melvin* and *Flotron* noted these examples in denying motions to dismiss. Such an approach gives trial courts, in the first instance, the opportunity to recognize the outlines of a fraudulent scheme even in the absence of materially false statements and representations.

V. Other advantages in the use of section 1348(1)

As discussed above, section 1348(1) offers prosecutors a means to reach schemes to defraud in which the evidence of clear material misrepresentations is lacking. This will allow prosecutors to reach market manipulation cases, including "pump and dump" and spoofing schemes, as well as fraud schemes that involve registered securities, commodities for future delivery, or commodities options, where the conduct at issue was undertaken with the requisite intent to defraud. Such an approach affords prosecutors greater latitude in both charging and proving these cases.

The statute offers other advantages beyond the specific legal issue discussed above. The case law surrounding section 1348 offers prosecutors the opportunity for something of a fresh start in interpreting a securities fraud statute. Section 10b-5, for all of its versatility, has been interpreted so extensively that the case law underlying it is, at times, unhelpful to the government. Bad cases make bad law, and section 10b-5—which has been utilized extensively in civil securities fraud actions for decades, some of which have been frivolous or ill-taken—has spawned a wide variety of cases across the circuits which can cause confusion for prosecutors and judges alike. Section 1348, both because of its newness and the lack of a civil cause

of action, offers a simpler approach, without the unwelcome freight which decades of litigation—much of it civil—has piled onto 10b-5. Furthermore, for judges who rarely encounter securities fraud cases, section 1348's simplicity is an added benefit.

Section 1348 offers other benefits when compared with 10b-5. To violate section 1348, a defendant must act "knowingly" and with the intent to defraud, while criminal 10b-5 prosecutions require proof of "willfulness."[29] Willfulness generally requires the government to prove that the defendant acted with knowledge that the conduct was specifically unlawful.[30] By contrast, section 1348 merely requires, as with the mail and wire fraud statutes "fraudulent intent [which] may be inferred from the scheme itself."[31] In this way, the mens rea required to prove a violation of section 1348(1) appears to be lower than a criminal violation of 10b-5.[32]

Section 1348, in the context of securities fraud prosecutions, also omits the Rule 10b-5 requirement that the scheme be "in connection with the *purchase* or *sale* of a security,"[33] instead requiring only a connection to either (a) a registered security or (b) security of an issuer required to file reports under the Securities Exchange Act. Although courts have read this 10b-5 requirement broadly, by unmooring securities fraud from transactions themselves under section 1348, Congress broadened the scope of what could be covered under the statute by not limiting it solely to conduct that implicates purchases and sales. Virtually any fraud scheme which involves a

---

[29] 15 U.S.C. § 78ff(a).

[30] *See*, *e.g.*, Ratzlaf v. United States, 510 U.S. 135, 136–37 (1994) (the "willfulness" requirement mandates something more . . . "the Government must prove that the defendant acted with knowledge that his conduct was unlawful.").

[31] United States v. Motz, 652 F. Supp. 2d 284, 296 (E.D.N.Y. 2009) (citing United States v. D'Amato, 39 F.3d 1249, 1257 (2d Cir.1994)).

[32] This is consistent with congressional intent. *See* COMM. ON THE JUD., THE CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY ACT OF 2002, 107TH CONG., S. REP. 107-146, at 6 (2002). ("[P]rosecutors may charge a willful violation of certain specific securities laws or regulations, but such regulations often contain technical legal requirements, and proving willful violations of these complex regulations allows defendants to argue that they did not possess the requisite criminal intent. There is no logical reason for imposing such awkward and heightened burdens on the prosecution of criminal securities fraud cases.").

[33] 17 C.F.R. § 240.10b-5 (emphasis added).

registered security or the security of an issuer required to file reports with the Securities and Exchange Commission (SEC)—for example, a publicly traded company, and other entities which issue securities to a substantial number of investors—can be prosecuted under section 1348.

Finally, pursuing charges under section 1348 offers practical benefits. Unlike the mail and wire fraud statutes, section 1348 is subject to a six year statute of limitations, which offers prosecutors the ability to pursue charges later.[34] Section 1348 may also offer prosecutors a clearer road to venuing cases in their districts, without having to find interstate wires or mailings in furtherance of the scheme that occurred in specific locations. And section 1348 carries a stiffer maximum penalty—25 years of imprisonment—than the mail and wire fraud, 10b-5, and Title 7 statutes.[35]

Yet charging cases under section 1348 is not a panacea and does present some challenges for prosecutors. First, section 1348 is limited to conduct that has a nexus to one of two categories of financial products: registered securities, securities of an issuer required to file reports with the SEC, and commodities futures and options. This reading is far more circumscribed than, for example, the expansive Title 15 definition of "security."[36] In cases where the underlying security is unregistered or not issued by a company required to file reports with the SEC, section 1348 will not apply, and prosecutors will have to rely either on a 10b-5 theory or on the mail and wire fraud statutes in order to pursue a prosecution.

Second, section 1348's relative youthfulness means that the number of courts that have authoritatively interpreted it is still comparatively small. No circuit has yet promulgated pattern jury instructions for section 1348(1), and there is a lack of precedential case law

---

[34] 18 U.S.C. § 3301(b). The six year limitations period also applies to some securities fraud prosecutions conducted under Title 15, but does not apply to commodities fraud prosecutions pursuant to Title 7, or wire and mail fraud schemes affecting securities.

[35] The maximum penalty for a violation of 18 U.S.C. § 1348 is 25 years imprisonment. The maximum penalty for a violation of the mail and wire fraud statutes, or for 10b-5 securities fraud, is 20 years imprisonment. 18 U.S.C. §§ 1341, 1343; 15 U.S.C. § 78ff(a). The maximum penalty for a violation of the Title 7 commodities fraud statute is ten years imprisonment. 7 U.S.C. § 13(a).

[36] *See* 15 U.S.C. § 77b(a)(1) (defining "security" broadly).

interpreting the statute outside the Second and Seventh Circuits.[37] This may give prosecutors outside those circuits some pause, as it offers district and appellate courts the opportunity to shape the statute's interpretation going forward.

Given the relative newness of the statute, prosecutors charging securities fraud under section 1348(1) must educate courts about the statute, and the existing case law surrounding it, during the course of their cases. Failure to do so runs the risk of inadvertently creating bad case law.[38] The Fraud Section's Securities and Financial Fraud (SFF) Unit, home to over 40 prosecutors who specialize in securities, commodities, and other financial fraud, is a valuable resource for United States Attorneys' Offices and others in the Department. Prosecutors seeking to charge section 1348 cases should consult with the SFF Unit about legal developments, strategic approaches, and potential partnerships.

[37] In 2018, the District of South Carolina created a model jury instruction that distinguishes between section 1348(1) and (2). It may serve as a useful tool for prosecutors. *See* Eric Wm. Ruschky, *Pattern Jury Instructions for Federal Criminal Cases*, *District of South Carolina* § 1348 (2018 Online Edition).

[38] Some of the pattern instructions used in bank fraud cases offer an additional illustration of this potential problem. Even in circuits that have clearly articulated the principle that 18 U.S.C. § 1344(1) does not require false statements or representations, pattern jury instructions widely used throughout the circuit—and often blessed by the Court of Appeals and district judges alike—still insert a false statements requirement. *Contrast Third Circuit Model Criminal Jury Instructions* § 6.18.1344 (2017) (first element of bank fraud is scheme to defraud "by means of material false or fraudulent pretenses, representations or promises"), *with* Schwartz, *supra* note 9, at 246. Prosecutors should be careful that courts do not inadvertently combine the two subparts of section 1348, thus adding another legal requirement to the statute.

VI. Conclusion

Section 1348(1) offers prosecutors an opportunity to pursue market manipulation and other securities and commodities fraud cases without relying on material misrepresentations or omissions. Prosecutors should look to section 1348(1) when charging certain securities and commodities fraud cases under a broad "scheme to defraud" theory, where the underlying conduct was undertaken knowingly and with the intent to defraud.

About the Authors

Sandra Moser has led the Criminal Division's Fraud Section since the spring of 2017. Prior to assuming that role, Ms. Moser served in several leadership positions within the section, including Principal Deputy Chief. Prior to joining the Criminal Division, she was an Assistant United States Attorney in the district of New Jersey. Sandra is a graduate of Northwestern University school of Law.

Justin Weitz is an Assistant Chief in the Securities and Financial Fraud (SFF) Unit of the Fraud Section. Previously, he served as a Trial Attorney in the SFF Unit and in the Department's Public Integrity Section. He is a graduate of NYU Law School.

Responding to the Upward Trend of Multijurisdictional Cases: Problems and Solutions

Daniel Kahn
Chief
Foreign Corrupt Practices Act Unit
Fraud Section
Criminal Division

I. Introduction

As the economy has become increasingly global, and as more companies continue to expand their footprint across borders, white collar crime likewise has become more frequently multinational. These cases now routinely involve not only multiple United States enforcement agencies, but also one or more foreign authorities.

This development has had a significant positive impact on United States criminal cases because prosecutors are much more likely to secure evidence from overseas, and to be able to do so more quickly, when the relevant foreign authorities are themselves investigating the same or overlapping conduct and cooperating with United States authorities. The involvement of foreign authorities also means that criminals are less able to skirt prosecution by hiding themselves and evidence outside of the United States. Multinational cases, however, also pose a number of issues and obstacles for U.S. prosecutors to overcome.

This article addresses the upward trend of multijurisdictional white collar cases, identifies the issues attendant to that trend, and offers several ways of dealing with those issues. Because Foreign Corrupt Practices Act (FCPA) investigations and prosecutions, by their very nature, involve evidence from abroad in every case and often include multiple foreign authorities, such cases will be used to highlight these points.[1]

[1] The FCPA, 15 U.S.C. § 78dd-1, *et seq.*, prohibits the offer, promise, authorization, or payment of anything of value to a foreign official for the purpose of obtaining or retaining business.

II. Increased multijurisdictional cases

Over the past several years, there has been a significant uptick in activity by foreign authorities in the investigation and prosecution of white collar crime. This upward trend has been particularly conspicuous in the context of transnational corruption. Over the past several years, a number of countries successfully resolved their first corporate foreign bribery case, and a number of countries have coordinated resolutions with the Department of Justice, Criminal Division, Fraud Section's FCPA Unit.[2] In fact, since 2016, the Department has coordinated resolutions with foreign authorities in nine cases, which is more than twice as many as all previous years combined. Even where the Department did not coordinate resolutions in a particular case, the Department received significant cooperation from approximately 20 different countries in FCPA cases in 2017 alone.[3]

---

[2] Press Release, U.S. Dep't of Justice, 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) (noting that VimpelCom first coordinated resolution with the Dutch Prosecution Service); Press Release, U.S. Dep't of Justice, Embraer Agrees to Pay More than $107 Million to Resolve Foreign Corrupt Practices Act Charges (Oct. 24, 2016) (noting that Embraer first coordinated resolution with Brazil); Press Release, U.S. Dep't of Justice, 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) (noting that Odebrecht and Braskem first coordinated resolution with Switzerland); Press Release, U.S. Dep't of Justice, 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) (noting that Telia first coordinated with Sweden); Press Release, U.S. Dep't of Justice, 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) (noting that Keppel first coordinated with Singapore); Press Release, U.S. Dep't of Justice, 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) (noting Société Générale first coordinated resolution with France).

[3] RELATED ENFORCEMENT ACTIONS: 2017, FOREIGN CORRUPT PRACTICES ACT, CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-fraud/case/related-enforcement-actions/2017 (last visited Oct. 16, 2018).

Cooperation in such cases can be formal or informal, and in some cases both. Formal cooperation often takes the form of a written request for evidence, usually pursuant to a treaty. Most commonly, prosecutors can resort to bilateral treaties—Mutual Legal Assistance Treaties (MLATs)—into which the United States has entered with a number of foreign countries. MLATs govern the process for requesting and receiving evidence, define the obligation and process for requesting and providing assistance, and have the force of law. MLAT requests are submitted through the Department's Office of International Affairs (OIA), and they sometimes must transit through diplomatic channels, ultimately arriving at a foreign country's Central Authority, which has the ability to execute the request. Even where there is not a bilateral treaty, prosecutors can seek evidence from a foreign country pursuant to the principle of reciprocity, or pursuant to a multilateral treaty, which are often the products of international conventions. There are a number of conventions to which a large number of countries are signatories.[4] The United Nations Convention Against Corruption and the Organization for Economic Cooperation and Development (OECD) Anti-Bribery Convention on Combating Bribery of Foreign Public Officials in International Business Transactions are two conventions often used in the FCPA context to seek evidence from abroad, and include signatories with which the United States does not have MLATs.[5] Such conventions also often offer U.S. authorities an opportunity to make requests at meetings with foreign authorities and ensure they are working to satisfy the requests.

Unlike formal cooperation, informal cooperation takes place on a law enforcement to law enforcement basis, and is often quicker than seeking and receiving evidence through formal channels. On the other hand, prosecutors should be mindful that information and materials that are obtained through informal means may not be admissible because, for example, it may not contain the necessary certifications to establish the authenticity of the evidence or fall within a hearsay exception. The providing country also may not want information and materials provided informally to be used in court. However, where foreign authorities are engaged and assisting through informal

[4] CRIMINAL RESOURCE MANUAL § 276.

[5] Office on Drugs and Crime, United Nations Convention Against Corruption (2004); *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (OCED 2011).

cooperation, this often allows prosecutors to make concurrent MLAT or other formal requests more expeditious and efficient. Once a foreign authority has informally provided information or materials, prosecutors can specify exactly what they are looking for in their formal transmission, such as identifying specific bank account records or information about specific individuals. Informal cooperation can also help law enforcement identify the appropriate point of contact within the foreign government, which will often expedite the satisfaction of the formal request.

In the absence of cooperation from a foreign authority—either formal or informal—it can be very difficult to obtain sufficient evidence to prosecute the culpable individuals and entities involved in the crime. There are, however, other avenues for obtaining evidence from overseas. One way to obtain such evidence, even in the absence of cooperation from the foreign authority, is through voluntary productions by the relevant individuals and entities. For example, cooperating third parties, including defendants, often agree to provide evidence from abroad to U.S. authorities. Likewise, corporations often produce evidence to the Department that is outside the subpoena power of a grand jury in an effort to secure cooperation credit under the U.S. Sentencing Guidelines (USSG) and Justice Manual.[6]

Due to the inherently international character of FCPA cases, the Department has sought to provide additional incentives and benefits to companies that fully cooperate in such cases.[7] Where a company voluntarily self-discloses misconduct and fully cooperates with the Department's investigation, and then remediates the misconduct, there is a presumption that the company will receive a declination in the absence of aggravating circumstances.[8] Even where the company does not voluntarily self-disclose the misconduct, but nevertheless

---

[6] *See, e.g.,* U.S. SENTENCING GUIDELINES § 8C2.5(G) (U.S. SENTENCING COMM'N 2015) (providing that a company's full cooperation will reduce the culpability score that determines the appropriate fine under the USSG); *see also* JUSTICE MANUAL § 9-47.000 (referencing cooperation as a mitigating factor).

[7] JUSTICE MANUAL § 9-47.120 ("Due to the unique issues presented in FCPA matters, including their inherently international character and other factors, the FCPA Corporate Enforcement Policy is aimed at providing additional benefits to companies based on their corporate behavior once they learn of misconduct.").

[8] § 9-47.120(1).

cooperates and remediates, the company will receive, or the Department will recommend to a sentencing court, up to a 25% reduction off of the low end of the USSG fine range.[9] For purposes of this section of the Justice Manual, full cooperation is defined to include "[t]imely preservation, collection, and disclosure of relevant documents and information relating to their provenance, including (a) disclosure of overseas documents, the locations in which such documents were found, and who found the documents, (b) facilitation of third-party production of documents, and (c) where requested and appropriate, provision of translations of relevant documents in foreign languages."[10] In addition, when the cooperating company claims that it is unable to disclose certain overseas documents due to legal prohibitions, the Justice Manual provides that "the company bears the burden of establishing the prohibition," and "should work diligently to identify all available legal bases to provide such documents."[11]

Crediting companies for providing such overseas evidence incentivizes and rewards them for the production of documents that the Department may otherwise be unable to obtain or that would take much longer to obtain through formal cooperation.

Another way in which prosecutors can obtain evidence from abroad even in the absence of cooperation by foreign authorities is through a so-called *Bank of Nova Scotia* subpoena. Such subpoenas permit the grand jury to obtain evidence that a company maintains abroad by serving subpoenas on offices of the company located in the United States.[12] However, such compulsory process can cause issues with

---

[9] § 9-47.120(2) (noting that if a company does not meet all of the criteria for full cooperation, it is still eligible for some cooperation credit, although the credit generally will be markedly less than for full cooperation, depending on the extent to which the cooperation was lacking).

[10] § 9-47.120(3)(b).

[11] *Id.*

[12] *See In re* Grand Jury Proceedings the Bank of Nova Scotia, 740 F.2d 817, 826–27 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985) (rejecting bank's assertion that compliance with the U.S. grand jury subpoena would require it to violate the Cayman Islands' secrecy laws and upholding sanctions on bank for failing to comply with subpoena for records). *See also In re* Grand Jury Subpoena Dated August 9, 2000, 218 F.Supp.2d 544, 554 (S.D.N.Y. 2002) ("Courts consistently hold that the United States' interest in law enforcement outweighs the interests of the foreign states in bank secrecy and the hardships imposed on the entity subject to compliance."); *cf.*

foreign countries and can adversely affect the law enforcement relationship with those countries. As a result, prosecutors must consult with OIA before resorting to such subpoenas[13] and must consider factors such as the availability of alternative methods for obtaining the records in a timely manner, such as use of MLATs, the indispensability of the records to the success of the investigation or prosecution, and the need to protect against the destruction of records located abroad.[14] Courts likewise will balance the interests of both the United States and foreign country when determining whether to compel production pursuant to such a subpoena.[15] In addition to balancing the competing interests presented by such subpoenas and the relationship with foreign authorities, prosecutors should also consider whether the company being subpoenaed voluntarily disclosed the case and/or has been cooperating with the Department's investigation.[16] If, for example, a company has voluntarily disclosed the misconduct to the Department and is cooperating, prosecutors may choose not to place the company in the position of having either to violate a U.S. court order to compel production of the material or to violate the foreign law or regulation prohibiting such production, which may discourage companies from voluntarily disclosing such cases and cooperating.

Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 543–44 (1987) (holding that foreign country's blocking statute does not preclude U.S. court from ordering a party subject to the foreign jurisdiction to produce evidence even though the act of production may violate the foreign blocking statute).

[13] JUSTICE MANUAL § 9-13.525.

[14] CRIMINAL RESOURCE MANUAL § 279.

[15] *See, e.g.*, *Bank of Nova Scotia*, 740 F.2d at 827–29 (describing the interests that courts should consider in determining whether to compel production despite competing or inconsistent foreign law); *Grand Jury Subpoena*, 218 F. Supp. 2d at 554 ("When the laws of two jurisdictions conflict, the court must balance the interests, including the respective interests of the states involved and the hardship that would be imposed upon the person or entity subject to compliance.").

[16] *See* JUSTICE MANUAL §§ 9-47.120, 9-28.000.

III. Issues that arise in multijurisdictional cases

Despite the clear benefits of working on multinational cases with foreign authorities, there are also a number of obstacles and issues attendant to such cases.

One such issue is that some foreign countries have distinct laws and regulations that permit foreign prosecutors to engage in investigative techniques that are prohibited under U.S. law or constitutional principles. For example, certain jurisdictions, including the United Kingdom, permit criminal authorities to compel testimony even where the witness is not granted full (including derivative) immunity.[17] Even where U.S. prosecutors take precautions to prevent such compelled testimony from infiltrating its case, if the U.S. prosecutors or witnesses in the case become exposed to such compelled testimony, it may prevent the prosecution of the compelled individual.[18]

Another issue that arises in multijurisdictional cases is the inability of U.S. prosecutors to obtain evidence from abroad due to data privacy restrictions, blocking statutes, or State secrecy laws. Data privacy laws, in general, restrict the transfer of personal data or the sourcing of personal data, and thus would likely inhibit a cooperating company from disclosing certain information to U.S. prosecutors.[19] Companies may be able to overcome such data privacy restrictions by obtaining permission to share information from the employees whose privacy is implicated. Many countries would also produce the information pursuant to an MLAT or other formal request. It may also be possible for the company to produce redacted versions of the materials while these processes are underway.

---

[17] Criminal Justice Act 1987, § 2.

[18] *See* United States v. Allen, 864 F.3d 63 (2d Cir. 2017) (holding that indictment against defendant must be dismissed because cooperating witness was exposed to defendant's compelled testimony and government could not overcome *Kastigar* burden to demonstrate that such exposure did not taint the witness's testimony).

[19] *See, e.g.*, THE GENERAL DATA PROTECTION REGULATION APPLIES IN ALL MEMBER STATES FROM 25 MAY 2018, EUR-LEX, https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html (last visited Oct. 16, 2018).

Blocking statutes, by contrast, are often aimed at protecting some interest of the foreign country, not of the individuals in those countries, and thus sometimes may not be overcome through waiver or even MLAT requests. For example, the French blocking statute prohibits the provision of evidence to foreign authorities (including the United States) if that evidence implicates the economic, commercial, industrial, financial, or technical interests of France, unless the evidence is obtained through the Hague convention.[20]

Where U.S. prosecutors are unable to secure evidence voluntarily or through formal requests to foreign countries due to data privacy laws or blocking statutes, there may be circumstances where the evidence can be obtained through compulsory process, including the *Bank of Nova Scotia* subpoenas discussed above.

Yet another issue that is implicated by multijurisdictional cases is when multiple countries intend to prosecute the same individuals or entities. The Justice Manual provides guidance for how prosecutors should determine whether to initiate or decline prosecution where another jurisdiction is also prosecuting.[21] These factors include: (1) the strength of the other jurisdiction's interest in prosecution; (2) the other jurisdiction's ability and willingness to prosecute effectively; and (3) the probable sentence or other consequences if the person is convicted in the other jurisdiction.[22]

Where U.S. prosecutors determine that it is appropriate to prosecute an individual or company despite the fact that a foreign authority is also doing so, it is important to attempt to coordinate with the foreign authority to ensure the greatest likelihood of successfully apprehending the individual and to secure the most just resolution with the individual or entity. Prosecution of individuals by multiple sovereigns poses certain logistical and constitutional issues that are not as glaring in cases involving corporations. For example, an individual cannot be present for a trial in the United States if he or she is being tried in a foreign country and is then sentenced to a

---

[20] *See* Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères (Law n° 68-678 of July 26, 1968 relating to the communication of documents and information of an economic, commercial, industrial, financial or technical nature to physical or legal foreign persons).

[21] *See* JUSTICE MANUAL § 9-27.240.

[22] *Id.*

number of years in prison in that country. Accommodations or agreements may be reached with a foreign country to permit the extradition of an individual after trial and sentencing in the foreign country but before the defendant begins serving his or her sentence. A corporation, on the other hand, may stand trial in multiple jurisdictions and have corporate representatives present at each trial, and a corporation obviously is not sentenced to a term of imprisonment, but rather to pay a fine, restitution, and/or disgorgement.[23]

IV. The benefits of coordinating resolutions in multijurisdictional cases

In a growing number of cases corporations that are under investigation in multiple countries are reaching criminal resolutions with authorities in those countries. The Deputy Attorney General recently announced a revision to the Justice Manual that encourages Department attorneys to not only coordinate with one another but also with other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct, and to consider the amount of fines, penalties, or forfeiture paid to such authorities.[24] Prosecutors are to consider "all relevant factors in determining whether coordination and apportionment between Department components and with other enforcement authorities allows the interests of justice to be fully vindicated," including "the egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department, separate from any such disclosures and cooperation with other relevant enforcement authorities."[25]

In the transnational corruption context, the Department has routinely coordinated resolutions with the U.S. Securities and Exchange Commission (SEC), wherein the Department imposes a criminal fine or penalty, and the SEC disgorges the profits from the

---

[23] *See, e.g.*, Melrose Distillers, Inc. v. United States, 359 U.S. 271, 274 (1959) ("[A] corporation cannot be sent to jail. The discharge of its liabilities whether criminal or civil can be effected only by the payment of money.").
[24] *See* JUSTICE MANUAL § 1-12.100.
[25] *Id.*

illegal scheme. In such cases, the Department credits the disgorgement paid to the SEC, and the SEC credits the penalty imposed by the Department.[26] More recently, the Department has coordinated resolutions with a number of foreign authorities, including Brazil, France, the Netherlands, Singapore, Sweden, Switzerland, and the United Kingdom.[27]

Coordinating resolutions, where appropriate, accomplishes several important objectives, benefiting the company, U.S. interests, and our foreign counterparts. First, crediting fines, penalties, and/or disgorgement treats companies fairly, and does not increase the

---

[26] *See, e.g.*, Non-Prosecution Agreement at pp.4–5, General Cable Corp., U.S. Dep't of Justice Dec. 22, 2016); Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order at p.11 ¶¶ 53–54, In re General Cable Corp., No. 3-17755 (SEC Dec. 29, 2016).

[27] Press Release, U.S. Dep't of Justice, 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) (noting that VimpelCom first coordinated resolution with the Dutch Prosecution Service); Press Release, U.S. Dep't of Justice, Embraer Agrees to Pay More than $107 Million to Resolve Foreign Corrupt Practices Act Charges (Oct. 24, 2016) (noting that Embraer first coordinated resolution with Brazil); Press Release, U.S. Dep't of Justice, 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) (noting that Odebrecht and Braskem first coordinated resolution with Brazil and Switzerland); Press Release, U.S. Dep't of Justice, 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) (noting that Telia first coordinated with Sweden and the Dutch); Press Release, U.S. Dep't of Justice, 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) (noting that Keppel first coordinated with Singapore and Brazil); Press Release, U.S. Dep't of Justice, 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) (noting Société Générale first coordinated resolution with France); Press Release, U.S. Dep't of Justice, Petróleo Brasileiro S.A.-Petrobras Agrees to Pay More Than $850 Million for FCPA Violations (Sept. 27, 2018) (noting that Petrobras coordinated resolution with Brazil); Press Release, U.S. Dep't of Justice, Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case (Jan. 17, 2017) (noting that Rolls-Royce coordinated resolution with U.K. and Brazil).

monetary amount paid by the company based solely on the number of enforcement authorities involved. In essence, the various authorities determine what the appropriate monetary sanction should be in a particular case, and that is the total amount paid by the company, with the authorities deciding what amount each of them will take. This avoids the "piling on" phenomenon, whereby the company faces duplicative monetary sanctions for the same conduct.

Second, because coordinating resolutions and crediting amounts paid to other jurisdictions benefits a company by avoiding duplicative penalties, doing so also incentivizes cooperation and voluntary self-disclosures by companies. Put another way, where a company discovers misconduct and is making the determination of whether to voluntarily self-disclose the misconduct and/or cooperate with the government's investigation, one factor that the company will inevitably weigh is whether doing so will increase the chances that it will face sanctions in multiple jurisdictions and whether those sanctions will be coordinated or not. As discussed above, in cases involving significant overseas evidence, cooperation by a company can make the Department's investigation much more expeditious and effective.

Third, a number of foreign countries have double jeopardy, or *non bis in idem*, laws that prohibit the prosecution of a company or individual twice for the same crime. Thus, if U.S. prosecutors do not coordinate resolutions, it is very possible that the foreign country may be precluded from bringing a case.

Once U.S. prosecutors decide to coordinate with foreign authorities, the coordinating authorities must decide how to credit one another. For example, one jurisdiction can impose the criminal penalty and the other can impose disgorgement, much like the Department does with the SEC in a number of cases. Alternatively, once an appropriate penalty amount is determined, the jurisdictions can divide that amount and credit the remaining amount to the other jurisdiction(s).

In determining how much to credit a particular jurisdiction, there are a number of factors that the FCPA Unit has found instructive, including where the illegal conduct took place, where the harm occurred, where the victims reside, the headquarters of the relevant entities and the nationality of culpable individuals, which jurisdiction initiated the investigation, and the time and resources expended by each jurisdiction.

For example, in *United States v. Odebrecht S.A.*, a global construction conglomerate based in Brazil engaged in a widespread

scheme to pay hundreds of millions of dollars in bribes to government officials around the world. The investigation was initiated by Brazilian authorities, Brazilian authorities expended significant time and resources on the case, and much of the scheme took place in Brazil. In addition to Brazil, however, the co-conspirators took significant acts in the United States and Switzerland. Many of the bribes were laundered through Swiss financial institutions. A number of the offshore entities used to hold and disburse the bribes were established, owned, and/or operated by individuals located in the United States, and two Odebrecht employees engaged in the scheme, including holding meetings and moving criminal proceeds, in the United States.[28] Because the majority of the conduct took place in Brazil, and because Brazil otherwise had significant equities implicated by the case, Switzerland and the United States agreed to credit 80% of the fine to Brazil, and divided the remaining 20% evenly among them.[29]

By contrast, taking these factors into consideration, the Department coordinated resolutions in several cases where the U.S. credited 50% of the resolution to foreign countries.[30]

Despite the significant benefits for the Department, foreign authorities, and company in reaching a coordinated resolution, there may be occasions where it is not appropriate to do so, or where it is simply not possible. For example, a foreign authority may be unwilling to coordinate with the United States to reach such a resolution. Or, a foreign authority may choose not to investigate a case and instead seek to "pile on" a Department resolution once the resolution is announced. Likewise, some companies may attempt to silo the various investigative authorities and would rather fight each authority than reach a voluntary and coordinated resolution. In determining whether it is appropriate to coordinate with foreign

---

[28] Information, United States v. Odebrecht S.A., No. 16-643-RJD (E.D.N.Y. 2016).

[29] Plea Agreement at ¶ 21, United States v. Odebrecht S.A., No. 16-643-RJD (E.D.N.Y. 2016).

[30] *See, e.g.*, Deferred Prosecution Agreement, United States v. Société Générale S.A., No. 18-CR-253-DLI (E.D.N.Y. June 5, 2018).; Deferred Prosecution Agreement at ¶ 7, United States v. VimpelCom Ltd., No.16-cr-137-ER (S.D.N.Y. Feb. 22, 2016), ECF No. 6; Deferred Prosecution Agreement at ¶ 7, United States v. Telia Company AB, No. 17-cr-581-GBD (S.D.N.Y. Sept. 21, 2017), ECF No. 6.

authorities and credit amounts paid to those authorities, U.S. prosecutors should consider "[t]he egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department, separate from any such disclosures and cooperation with other relevant enforcement authorities."[31]

V. Conclusion

Multijurisdictional cases offer prosecutors a significant opportunity to obtain evidence they likely would not be able to secure, and as a result to build better cases. Coordination with foreign authorities also ensures that the culpable individuals and entities are more likely to be apprehended and prosecuted for their crimes.

This upside, however, can come at a cost, and prosecutors should be mindful of the issues that surface in these types of cases. Although there is no "silver bullet" to address these issues, there are steps, as described in this article, that U.S. prosecutors can take to minimize the risk to their case. The law in these types of cases is continuing to develop, but one thing appears certain—with the significant increase in multinational crimes and the corresponding increase in multijurisdictional cases such issues are here to stay, and likely new ones will continue to emerge.

About the Author

Daniel Kahn has been with the Department of Justice, Criminal Division, Fraud Section since 2010, was an Assistant Chief in the Foreign Corrupt Practices Act (FCPA) Unit from 2013 to March 2016, and has been the Chief of the FCPA Unit since that time. He earned the Assistant Attorney General's Award for Exceptional Service for his work on the Alstom case, and the Assistant Attorney General's Award for Distinguished Service for his part in prosecuting a bribery scheme involving the state-owned and state-controlled telecommunications company in Haiti. He received his B.S. from Cornell University and J.D. from Harvard Law School.

[31] JUSTICE MANUAL § 1-12.100.

Page Intentionally Left Blank

Asset Forfeiture and Corporate Offenders

Curt Bohling
Assistant United States Attorney
Chief, Appellate Unit (formerly Chief, Monetary Penalties Unit)
United States Attorney's Office
Western District of Missouri

I. Introduction

The asset forfeiture tools furnished by Congress provide federal prosecutors with the ability to "confiscate assets used in or gained from certain serious crimes."[1] Asset forfeiture serves to punish the wrongdoer, deter future illegality, lessen the economic power of criminal enterprises, compensate victims, improve conditions in crime-damaged communities, and support law enforcement activities such as police training.[2]

Prosecutors face a wide array of challenges when utilizing asset forfeiture remedies where corporate entities are involved. Where the corporate entity involved is an established business, prosecutors should balance the goals and benefits of asset forfeiture with "the thoughtful analysis of all facts and circumstances presented in a given case," recognizing "that corporate prosecutions can potentially harm blameless investors, employees, and others."[3] Prosecutors also have an obligation to coordinate the use of asset forfeiture enforcement with any existing or potential parallel proceedings seeking fines, penalties, or forfeiture for the same misconduct.[4] Section II discusses the use of asset forfeiture consistent with the Department of Justice's principles of federal prosecution of corporate entities.

[1] Kaley v. United States, 571 U.S. 320, 323 (2014).
[2] *Id.* (quoting Caplin & Drysdale, Chartered v. United States, 491 U.S. 617, 630 (1989)).
[3] JUSTICE MANUAL § 9-28.100.
[4] § 1-12.100.

II. Asset forfeiture and the principles of federal prosecution of business organizations

A. Department of Justice guidance concerning the federal prosecution of business organizations and the use of asset forfeiture

Federal prosecutors investigating corporate misconduct are often faced with difficult charging decisions. Criminal charges may promote critical public interests by protecting the integrity of our economic and capital markets, as well as consumers, investors, and competing businesses.[5] However, criminal prosecution of a corporate entity may also affect the interests of blameless employees and investors, and undermine public confidence in the prosecutor's exercise of discretion.[6] To assist federal prosecutors in making charging decisions, the Department of Justice has formulated "Principles of Federal Prosecution of Business Organizations," found in the Justice Manual at § 9-28.000. The Principles were last updated in November 2015.

Justice Manual § 9-28.300 lists nine non-exclusive factors a prosecutor should consider when determining how to treat a corporate target.[7] These factors include the nature and seriousness of the offense, the pervasiveness of the wrongdoing within the corporation, the corporation's willingness to cooperate in the investigation and its timely disclosure of the wrongdoing, and the collateral consequences of the decision to prosecute. Making restitution, or showing willingness to do so, is one of several types of remedial efforts a prosecutor may consider in the decision making process.[8] The prosecutor may also consider whether civil or regulatory alternatives to prosecution would adequately deter, punish, and rehabilitate a corporation if used in the stead of criminal charges.[9]

Asset forfeiture occupies a unique niche within the guidelines articulated by the Principles. On the one hand, asset forfeiture, either criminal or civil, may occur in conjunction with a criminal prosecution. On the other hand, civil asset forfeiture may be used as a freestanding

[5] § 9-28.100.
[6] *Id.*
[7] § 9-28.300.
[8] § 9-28.1000.
[9] § 9-28.1200.

remedy for the recovery of criminally derived assets, thereby serving as a civil alternative to criminal prosecution in an appropriate case.

In either case, asset forfeiture is a powerful remedy that must be balanced with any parallel financial penalties stemming from the same misconduct. To formalize the policy, in May 2018 the Deputy Attorney General announced a new section to be incorporated into Title 1 of the Justice Manual. New Justice Manual § 1-12.100 governs the "Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct." The section begins by reminding Department attorneys that they "should remain mindful of their ethical obligation not to use criminal enforcement authority unfairly to extract, or to attempt to extract, additional civil or administrative monetary payments." The goal of Department attorneys should be to achieve "an equitable result" by taking into consideration the total overall financial penalties to be exacted in every parallel proceeding, not just the matter being prosecuted by that Department component.

Section 1-12.100 provides common examples of the coordination efforts expected of Department attorneys. Initially, Department components may need to coordinate with each other where Department attorneys are investigating the same misconduct. As a common example, a United States Attorney's Office may have an open investigation in which criminal or civil forfeiture enforcement is a possible outcome. At the same time, one of the civil components of the Department may have a False Claims Act civil action open on the same or closely related alleged misconduct, either as a filed case or as an investigation. Often these cases are filed by qui tam relators and will be kept under seal while the government investigates the claim. Quite commonly, the False Claims Act case will have been filed in a jurisdiction other than the one in which the criminal investigation is occurring. Section 1-12.100 requires coordination of the Department attorneys handling these related investigations to insure that the combined fines, penalties, and forfeitures demanded of the corporate entity are equitable in their totality.

Section 1-12.100 also directs Department attorneys to endeavor, as appropriate, to coordinate with other federal agencies as well as state, local, and foreign enforcement authorities. Many federal agencies have the ability to assess fines and penalties themselves, or to bring

civil judicial actions seeking fines, penalties, or judgments.[10] States and foreign authorities may have innumerable criminal, civil, and administrative avenues for compensating victims, forfeiting assets, or assessing fines and penalties, to include actions by state Attorney General's Offices, state securities or consumer focused regulatory agencies, and foreign antitrust enforcement authorities.

When initiating coordination efforts in accordance with Justice Manual § 1-12.100, Department attorneys must be mindful of the legal and ethical constraints associated with the conduct of parallel proceedings. The courts have recognized that parallel civil and criminal proceedings are both appropriate and constitutional.[11] Indeed, it is incumbent upon Department attorneys to be aware of both existing and potential parallel proceedings, as well as the possible financial resolutions of each proceeding, in order to resolve the criminal and civil forfeiture outcomes to comply with Justice Manual § 1-12.100's requirement to achieve an equitable result by considering all related financial recoveries and penalties to be assessed for the same misconduct.

However, when coordinating with other Department of Justice components or non-Department of Justice entities, Department attorneys must strive to do so appropriately. Of course, it can be very helpful to conduct "global" settlement negotiations with a corporate entity in which all of the agencies or jurisdictions involved seek to resolve all claims against the corporate entity in tandem. However, as a matter of legal ethics, counsel for the corporate entity must request global discussions.[12] Such requests by the government may be

---

[10] For example, the Securities and Exchange Commission can assess administrative penalties against corporate entities. The penalties range from $50,000 to $500,000 per occurrence of a violation. 15 U.S.C. § 78u-2. The Federal Deposit Insurance Corporation assesses civil monetary penalties pursuant to 12 U.S.C. § 1818, among other statutes.

[11] United States v. Kordel, 397 U.S. 1, 11 (1970); *see also* Securities & Exch. Comm'n v. Dresser Indus., Inc., 628 F.2d 1368, 1377 (D.C. Cir. 1980) ("Effective enforcement of the securities laws requires that the SEC and [the Department of] Justice be able to investigate possible violations simultaneously.").

[12] ABA STANDARDS ON PROSECUTORIAL INVESTIGATIONS § 2.13(c) ("A prosecutor should consider the appropriateness of non-criminal or global (civil and criminal resolutions) dispositions *suggested by subjects or targets*, whether or not they choose to cooperate, and may consider *proposals by them*

perceived as improperly coercive. Fortunately, sophisticated private counsel are generally aware of this requirement and will initiate global settlement discussions in an appropriate manner.

In addition, Department attorneys must conform their actions to ethical rules and Department policies relevant to parallel proceedings and global resolutions. Criminal prosecutors should not guide parallel civil actions to gather evidence for the criminal case, and especially not covertly.[13] Nor is it appropriate to reduce or eliminate criminal exposure in exchange for payment of a financial penalty, or to lessen an otherwise appropriate financial penalty in exchange for a plea to criminal charges, solely to coerce an outcome,[14] although it is both permissible and encouraged to evaluate the adequacy of non-criminal alternatives on their merits when considering whether to criminally charge a corporate entity.[15] Finally, Department attorneys cannot bind other United States Attorney Offices without the approval of the other district's United States Attorney or the appropriate Assistant Attorney General.[16]

Implementing Justice Manual § 1-12.100 in the context of parallel proceedings can mean negotiating a series of complex hurdles, including identifying both the actual and potential parallel proceedings, communicating and coordinating with those conducting parallel proceedings in an appropriate and ethical manner, and appropriately balancing the criminal and civil interests of each proceeding within the context of the Department's guidance on the

---

to include civil or regulatory sanctions as part of a disposition or cooperation agreement.") (emphasis added).

[13] United States v. Scrushy, 366 F. Supp. 2d 1134 (N.D. Ala. 2005) (charges dismissed against a CEO because district court concluded there had been improper consultations between Department of Justice attorneys and SEC attorneys before a deposition).

[14] JUSTICE MANUAL § 9-113.106 ("Settlement of Forfeiture in Conjunction With Plea Bargaining," provides that: "The Department does not release property which is otherwise subject to forfeiture to encourage guilty pleas; nor does it permit defendants to submit property which is otherwise not subject to forfeiture in order to lighten the potential incarceration component of the punishment."); *see* Town of Newton v. Rumery, 480 U.S. 386, 400–401 (1987) (agreement to drop charges in exchange for a release of civil claims enforceable, but may result in having to determine whether there are any ethical concerns).

[15] JUSTICE MANUAL § 9-28.1200.

[16] JUSTICE MANUAL § 9-27.641.

prosecution of corporate organizations. The next section discusses a recent example of a case in which Department attorneys successfully negotiated these hurdles to reach an appropriate and equitable resolution for a corporate entity facing parallel proceedings.

B. U.S. Bancorp deferred prosecution agreement and resolution of parallel civil proceedings

U.S. Bancorp is a bank holding company and the parent company of U.S. Bank, a well-known national bank and the fifth largest bank in the United States. In February 2018, U.S. Bancorp entered into a deferred prosecution agreement, or DPA, with the United States Attorney's Office for the Southern District of New York to resolve allegations that U.S. Bank willfully failed to maintain an adequate anti-money laundering (AML) program as required by Title 31 of the United States Code.[17] In reaching this agreement, the United States Attorney's Office coordinated the outcome of the civil forfeiture action with parallel civil money penalty actions by federal bank and financial regulators. The resolution is exemplary of the type of coordination envisioned by section 1-12.100.

Financial institutions like U.S. Bank have a legal obligation to file Suspicious Activity Reports, or SARs, when the bank suspects a criminal violation or other reportable event has occurred.[18] In April 2004, U.S. Bank made the decision to set a cap on the suspicious activity alerts generated by its anti-money laundering money system, even though testing revealed that the system was not reporting suspicious transactions.[19] The bank also did not hire sufficient AML staff to review and investigate suspicious activity, and did not follow through on feedback from its regulator, the Office of the Comptroller of the Currency (OCC).[20] These issues persisted at least through 2014.[21]

The issues with U.S. Bank's AML program came into focus when two of its largest customers became embroiled in federal criminal investigations. The first was the money transmitting business

---

[17] Deferred Prosecution Agreement, United States v. U.S. Bancorp (Feb. 12, 2018).
[18] 31 U.S.C. § 5318(g)(3); *see* Whitney Nat. Bank v. Karam, 306 F. Supp. 2d 678, 680 (S.D. Tex. 2004) (describing the federal SAR reporting requirement).
[19] Deferred Prosecution Agreement, *supra* note 17.
[20] *Id.*
[21] *Id.*

Western Union, which became a bank customer in 2009. In 2017, Western Union entered into a DPA with the Money Laundering and Asset Recovery Section of the Department of Justice and four United States Attorney's Offices.[22] The United States alleged that Western Union allowed its services to be used to facilitate numerous fraud schemes, and to move hundreds of millions of dollars to China for payment of human smuggling fees, among other suspected uses.[23] U.S. Bank took Western Union on as a customer without doing an initial risk assessment, and then failed to adequately monitor and investigate indications of fraud in Western Union transactions, many of which involved non-customers of the bank.[24]

The second problematic customer of the bank was Scott Tucker, who was convicted of criminal charges in the Southern District of New York in 2017 for activities arising from his payday lending activities.[25] These charges related to allegations that Tucker violated state usury laws and the federal Truth-in-Lending Act through the activities of his payday lending businesses. Despite internal findings that Tucker's activity was suspicious, the bank never filed a Suspicious Activity Report.[26]

As a result of the allegations concerning the failure of its anti-money laundering program, U.S. Bancorp faced financial penalties from the United States Attorney's Office, through civil forfeiture, and numerous federal regulatory agencies, including the OCC, the Federal Reserve, and FinCEN. By entering the DPA with the United States Attorney's Office, U.S. Bancorp agreed to a $528 million total penalty amount. However, this large forfeiture was coordinated with the other civil penalties exacted in the matter.

---

[22] Deferred Prosecution Agreement, United States v. The Western Union Company, No. 17-CR-00011-CCC (M.D. Pa. Jan. 19, 2017), ECF No. 3. The four offices were Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania, and the Southern District of Florida.

[23] Press Release, U.S. Dep't of Justice, Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits $586 Million in Settlement with Justice Department and Federal Trade Commission (Jan. 19, 2017).

[24] Deferred Prosecution Agreement, *supra* note 17.

[25] Press Release, U.S. Dep't of Justice, Scott Tucker and Timothy Muir Convicted at Trial for $3.5 Billion Unlawful Internet Payday Lending Enterprise (Oct. 13, 2017).

[26] Deferred Prosecution Agreement, *supra* note 17.

Initially, the DPA provided that U.S. Bancorp would be credited against the forfeiture with the amount of the civil penalty levied by the OCC, which was $75 million.[27] Separately, FinCEN assessed a $185 million civil penalty against the bank, but $115 million of that penalty was deemed satisfied by the Department of Justice forfeiture action.[28] The Federal Reserve also imposed a $15 million penalty. Thus, all but $85 million of the $375 million in civil penalties assessed by the non-regulators were subsumed in the Department of Justice forfeiture action, which was the largest financial penalty. The United States Attorney's Office pledged to use the forfeited funds to assist with victim restitution efforts, which represented another tangible benefit to the joint resolution.

The coordination in the U.S. Bancorp matter was aided by the fact that the involved agencies were all federal ones, and that an existing framework existed to assist with appropriately coordinating the forfeiture action with the other penalty assessments. The case also involved sophisticated private counsel, which aids in negotiating and resolving complex cases. Other cases may involve higher hurdles to complying with Department policy concerning an equitable resolution of all financial penalties. Coordination with state and foreign governments may pose greater challenges, and may require a "wait and see" approach to allow the other proceedings outcomes to finalize in order to appropriately factor them in to the resolution of the federal forfeiture action. The first imperative is to become aware of other actual or potential proceedings that may have to be considered under Justice Manual § 1-12.100.

III. Conclusion

As the U.S. Bancorp example illustrates, corporate investigations may result in large forfeitures and other financial penalties to adequately vindicate the government's interests and deter future wrongdoing. New Justice Manual § 1-12.100 requires that Department attorneys recognize these important interests and balance them where corporate misconduct gives rise to exposure to

---

[27] *Id.*

[28] ASSESSMENT OF CIVIL MONEY PENALTY, IN THE MATTER OF U.S. BANK NATIONAL ASSOCIATION, NO. 2018-01, 19 (FEB. 15, 2018), https://www.fincen.gov/sites/default/files/enforcement_action/2018-02-15/FinCEN%20U.S.%20Bank%20-%20Assesment%20-%20FinCEN%20review%202.14.18%20Final%20%283%29.pdf (last visited Oct. 16, 2018).

financial penalties from multiple Department components, federal regulatory agencies, and state and foreign governments. While the coordination involved in these matters can be time-consuming and complex, the outcomes gained by such coordination will ensure that the totality of the societal interest involved in addressing corporate misconduct is vindicated.

About the Author

Curt Bohling is an Assistant United States Attorney in the Western District of Missouri, in the Kansas City, Missouri, office. He is currently Chief of the Appellate Unit. From 2010 to 2018 he served as Chief of the Monetary Penalties Unit, and beginning in 2016 as a member of the national Asset Forfeiture Working Group. In Kansas City he has also served in the Computer Crime and Child Exploitation Unit and in the Civil Division. From 1992 to 1997, Assistant United States Attorney Bohling worked in the United States Attorney's Office for the District of Columbia, and from 1986 to 1992 he worked in the Office of the General Counsel of the Commodity Futures Trading Commission in Washington, D.C. Bohling received an Attorney's General Award in 2018, the Department of Homeland Security Director's Silver Medal Award in 2015, and an EOUSA Director's Award in 2004. He has taught numerous classes at the NAC on asset forfeiture, money laundering, legal ethics, and other topics. Assistant United States Attorney Bohling graduated from the University of Kansas School of Law in 1985, and from Emporia State University in 1982.

Page Intentionally Left Blank

Private Sector Honest Services Fraud Prosecutions After *Skilling v. United States*

Byung J. "BJay" Pak
United States Attorney
Northern District of Georgia

I. Introduction

One of the most powerful tools prosecutors have used to charge corporate officers and executives for corruption and undisclosed self-dealing is 18 U.S.C. § 1346—the theft of "intangible rights of honest services" prong of the mail and wire fraud statutes.[1] On June 24, 2010, the Supreme Court decided *Skilling v. United States*,[2] in which it limited the scope of section 1346 prosecutions to those cases involving only "bribes and kickbacks." The decision significantly changed the landscape of white collar prosecutions under the "intangible rights" theory.

This article examines honest services fraud prosecutions under section 1346 of private, non-public actors since *Skilling*, and how the courts have dealt with the remaining unanswered issues surrounding section 1346.

II. Brief history of the "Intangible Rights Theory" of the fraud statutes

First believed to be recognized in *Shushan v. United States*[3] in 1941, the "intangible rights" theory grew out of the various circuit courts' reading of the term "scheme or artifice to defraud" contained in the mail and wire fraud statutes to include deprivation of intangible rights, and not just money or property.[4]

In 1987, however, the Supreme Court rejected the "intangible rights" theory of mail and wire fraud by applying a plain language

[1] 18 U.S.C. § 1346.
[2] Skilling v. United States, 561 U.S. 358 (2010).
[3] Shushan v. United States, 117 F.2d 110 (5th Cir. 1941).
[4] McNally v. United States, 483 U.S. 350, 358 (1987); *Skilling*, 561 U.S. at 400.

interpretation of the statutes.[5] In *McNally v. United States*, the prosecutors brought charges against three individuals for a violation of the mail fraud statute under the theory that the defendants participated in a "self-dealing patronage scheme [which] defrauded the citizens and government of Kentucky" of the defendants' honest services.[6] The issue raised on appeal was whether the jury charge given at trial—which articulated the intangible rights to honest services theory of fraud—was permissible under the language of the federal mail fraud statute, 18 U.S.C. § 1341.

The Court stated that, although the "mail fraud statute clearly protects property rights, [it] does not refer to the intangible right of the citizenry to good government."[7] As such, the Court found that the intangible rights theory jury instruction "permitted a conviction for conduct not within the reach of § 1341,"[8] and overturned the convictions.

Shortly thereafter, Congress passed a new law, codified at 18 U.S.C. § 1346, specifically to overrule *McNally v. United States* and to restore the intangible rights theory to the wire and mail fraud statutes.[9] Section 1346 states: "For the purposes of this chapter, the term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services."[10] While in a rush to address the holding in *McNally*, Congress, unfortunately, did not provide clarification of the phrase "intangible right of honest services," where the victim's "right" to honest service is derived from, nor who is required to provide such honest services.

III. *Skilling v. United States*

Shortly after Congress enacted section 1346 in 1988, prosecutors continued using the honest services theory of wire/mail fraud to charge wide-ranging conduct[11] by individuals in the private sector who, in breach of their fiduciary duty to one another, enriched

[5] *See McNally*, 483 U.S. at 356.
[6] *Id.* at 352.
[7] *Id.* at 356.
[8] *Id.* at 361.
[9] *Skilling*, 561 U.S. at 404–05.
[10] 18 U.S.C. § 1346.
[11] *See generally*, *Skilling*, 561 U.S. at 418–21 (providing a survey of cases taking various approaches to applying honest services fraud statute (Scalia, J., concurring in part)).

themselves or others, either through bribery and kickbacks or through undisclosed self-dealing.[12] That was, of course, until the Supreme Court decided *Skilling v. United States* 22 years later.

In *Skilling*, Skilling and other executives of Enron were convicted of conspiring to commit securities fraud and deny the company and its shareholders their rights to the executives' intangible right of honest services.[13] Skilling challenged his conviction, arguing that section 1346 was unconstitutionally vague.[14] More specifically, he argued that the phrase "the intangible right to honest services" does not adequately define what behavior the statute bars, and that it permits arbitrary and discriminatory enforcement.[15]

The Court declined to strike down the statute in its entirety, but "saved" it by construing the statute's reach with a limiting principle. Since a "vast majority of [honest-services] cases involved offenders who, in violation of a fiduciary duty, participated in bribery kickback schemes . . ."[16] the Court held that the statute would not be unconstitutionally vague if its scope was limited only to the "bribe-and-kickback core of the pre-*McNally* case law."[17] Perhaps more significantly, the Supreme Court expressly rejected the government's argument that section 1346's scope should also cover "undisclosed self-dealing by a . . . private employee—that is, the taking of official action by the employee that furthers his own undisclosed financial interests while purporting to act in the interests of those to whom he owes a fiduciary duty."[18]

---

[12] *See id.* at 405 ("While the honest-services cases preceding *McNally* dominantly and consistently applied the fraud statute to bribery and kickback schemes—schemes that were the basis of most honest-services prosecutions—there was considerable disarray over the statute's applications to conduct outside of that core category.").

[13] *Id.* at 369.

[14] *Id.* at 399.

[15] *Id.* at 403.

[16] *Id.* at 407.

[17] *Id.* at 409.

[18] *Id.* at 410 ("We conclude that a reasonable limiting construction of § 1346 must exclude [conflict of interest] cases.").

IV. Did *Skilling* actually "save" the Honest Services Fraud Statute?

Although the *Skilling* decision had some immediate impact on pending section 1346 prosecutions, it had a greater impact on future prosecutions. First, unlike the events after *McNally*, legislation to amend the section 1346 language to restore the prosecutor's ability to charge non-disclosed conflicts of interests by private parties as "scheme or artifice to defraud" has stalled. Second, the ruling may have had a "chilling effect:" it seems the total number of defendants charged with violations of section 1346 has decreased since the Supreme Court handed down its decision.[19]

It is difficult to determine the exact reason for such a dramatic decline of the statute's use, particularly if, as the Supreme Court stated, the "core" pre-*McNally* cases involved "bribes and kickbacks." After all, for those "core cases," nothing has changed. The logical conclusion is that the "non-core" pre-*McNally* cases—that is, undisclosed self-dealing cases—may have comprised the vast majority of section 1346 cases. Further, other possible explanations for the decline in usage of section 1346 may be related to the continued uncertainty surrounding the statute's scope and the lack of uniformity of the courts' application of the statute. Prosecutors may view the use of section 1346 as risky in light of these issues, since these would subject any convictions obtained to future difficult legal challenges. Indeed, even after the decision in *Skilling,* defendants continued to challenge section 1346 on vagueness grounds—although with limited success. There are two main areas of concern to note.

First, as Justice Scalia highlighted in his concurring opinion in *Skilling,* there is substantial uncertainty as to the source and scope of the fiduciary duty that forms the basis of the "intangible right of honest services" under section 1346.[20] With respect to this "source of fiduciary duty" issue, the majority declined to directly provide guidance other than to state that in bribery and kickback cases, "the existence of a fiduciary relationship . . . was usually beyond

---

[19] An October 22, 2018 search of the terms "1346 and honest" in all federal courts on the Westlaw database shows that the number of reported criminal cases where 18 U.S.C. § 1346 was charged decreased from 483 cases for the period beginning on October 1, 2002 and ending on May 31, 2010, to 18 cases for the period beginning June 1, 2010 and ending July 31, 2018.

[20] *Skilling*, 561 U.S. at 421 (Scalia, J., concurring in part).

dispute[.]"[21] Although the Court provided examples of relationships which create a fiduciary duty—such as "public official-public," "employer-employee," and "union official-union member"—it did not adopt a categorical approach or provide further guidance to identify the source or scope of any fiduciary duty a prospective defendant owes the victim.[22]

Since *Skilling*, courts have generally declined to take a categorical approach in determining whether particular types of relationships in the non-public sector created a "fiduciary duty" to support an honest services fraud charge. For example, the Ninth Circuit adopted a definition of a fiduciary relationship that expanded the types of relationships which may satisfy the honest services fraud statute requirements beyond the ones listed in *Skilling*. In *United States v. Milovanovic,*[23] several public employees and two independent contractors, who were responsible for administering and issuing commercial driver's licenses, were convicted of "theft of honest services mail fraud" for fraudulently issuing licenses to unqualified drivers in exchange for money.[24]

The district court dismissed the superseding indictment against the defendants, holding that a formal fiduciary duty to the state and resulting economic harm were required to sustain a charge for honest services fraud.[25] In reinstating the section 1346 charges against the defendants, the Ninth Circuit provided some clarity with respect to the elements the government must prove to sustain an honest services fraud prosecution post-*Skilling*.

First, the *Milovanovic* court conclusively held that a breach of fiduciary duty was an element in an honest services mail fraud prosecution.[26] Second, the court explained that such a duty is not "limited to a formal 'fiduciary' relationship well-known in the law,"

---

[21] *Id.* at 407 n.41.

[22] In addition to the relationships identified by the Court in *Skilling*, other examples of relationships which indisputably create a fiduciary duty include: attorney-client; doctor-patient; stockbroker-customer; and real-estate broker-buyer. *See* United States v. Evans, No. 2:14-CR-00113, 2015 WL 1808904, at *5 (S.D.W. Va. Apr. 21, 2015) (citing United States v. Scanlon, 753 F. Supp. 2d 23, 25 (D.D.C. 2010); and United States v. Lupton, 620 F.3d 790, 804–05 (7th Cir. 2010)).

[23] United States v. Milovanovic, 678 F.3d 713 (9th Cir. 2012) (en banc).

[24] *Id.* at 716–17.

[25] *Id.* at 716.

[26] *Id.* at 722.

but also extends to a trusting relationship in which "one party acts for the benefit of another and induces the trusting party to relax the care and vigilance which it would ordinarily exercise."[27] The court expressly rejected the argument that a contractual label, such as "independent contractor," forecloses the existence of a fiduciary duty that was required and further held that the existence of a fiduciary duty was a factual question properly left for a jury.[28]

Other courts have looked to statutes (either state or federal) as sources to determine whether a non-public actor owed a "fiduciary duty" to its victims, and the scope of that duty. For example, in *United States v. Halloran*, Halloran was convicted for his participation in a scheme to bribe county Republican Party officials to provide their consent under a New York state law to allow a non-party member to run for office as a party member.[29] On appeal, the defendant raised an "as applied" void-for-vagueness challenge to his honest services fraud conviction by arguing that the government failed to specify the source of any fiduciary duty—for example, state law versus federal law—that the Republican party officials owed to the victims.[30] Finding that at the heart of the fiduciary relationship lies "reliance, and de facto control and dominance," the state law in question imposed such a duty, and that the "existence of a fiduciary duty is a question of fact for the jury,"[31] the Second Circuit found that

---

[27] *Id.* at 724 (citation omitted). *See generally,* Skilling v. United States, 561 U.S. 358, 417–24 (2010) (Scalia, J., concurring in part) (failing to adopt a categorical approach and adopting a fact-driven approach to define what types of relationships impose a "fiduciary duty" on a defendant for the purposes of an honest services fraud may lead to future due process challenges).

[28] *Milovanovic*, 678 F.3d at 725 ("We see no reason why [defendants] should be treated differently [from public employees] simply because the terms of their contracts label them independent contractors.").

[29] United States v. Halloran, 821 F.3d 321, 327–29 (2d Cir. 2016).

[30] *Id.* at 337–38.

[31] *Id.* at 339–40 ("The county chairs had de facto control over, and thus fiduciary duties to their party with respect to," Wilson-Pakulus law—the state law requiring party executive committee members to give their consent for a non-party member to run on the party's ticket.); *see also* United States v. Greenspan, No. CR 16-114 (WHW), 2016 WL 4402822, at *13–14 (D.N.J. Aug. 16, 2016) (finding that a New Jersey Medical Board rule against kickbacks created a fiduciary duty to defendant's patients).

there was sufficient evidence to support the conviction for honest services fraud.

Whether the existence of a fiduciary duty stems from one party who "acts for the benefit of another and induces the trusting party to relax the care and vigilance which it would ordinarily exercise," or who has "reliance and de facto control and dominance" over another, the courts undoubtedly will continue to debate exactly how and where the line between fiduciary duty and other relationships should be drawn. Regardless, there is a fair risk that any non-categorical definition of "fiduciary duty" may be so fact dependent that it fails to provide constitutional "fair notice" to the defendant. There are no reported cases ruling as such thus far.[32]

Another uncertain area related to honest services fraud prosecution involves what evidence is required to show harm to the victim. *Skilling* failed to bring forth a uniformity of approaches. Courts continue to split on whether the government needs to prove that the victim to whom a duty is owed suffered any economic harm, or that such harm was foreseeable to the defendant.

For example, in *United States v. Nayak*, the defendant, who owned multiple ambulatory surgery centers, made "under-the-table" payments to the physicians who referred patients to his centers.[33] Among other charges, the defendant was charged with honest services mail fraud. Nayak moved to dismiss the mail fraud count, "contending that the government needed to allege some form of actual or intended harm to the referring physicians' patients as an element of the crime."[34] The Seventh Circuit Court of Appeals rejected this argument and held that neither the statutory language of section 1346 nor its pre-*McNally* jurisprudence required a "showing of tangible harm to a

[32] Alleging and proving fiduciary relationships not "well-known in the law" can provide practical challenges in honest services fraud prosecutions. For example, once the district court rejected a plea to an information charging the defendant with honest services wire fraud because the government provided insufficient facts to show that the defendant—who was an employee of a subsidiary corporation—owed a fiduciary duty to the victim—the parent of the subsidiary corporation. *See* United States v. Evans, No. 2:14-CR-00113, 2015 WL 1808904, at *5 (S.D.W. Va. Apr. 21, 2015).

[33] United States v. Nayak, 769 F.3d 978, 979 (7th Cir. 2014).

[34] *Id.*

victim" as an element to support a violation of the honest services fraud statute.[35]

Likewise, the *Milovanovic* court rejected a similar argument and held that "[f]orseeable economic harm is not a necessary element when evaluating whether a party breached a fiduciary duty in violation of honest services fraud under §§ 1341 and 1346."[36] Instead, the Ninth Circuit court joined the Second, Fifth, Eighth, and Tenth Circuits in requiring that the misrepresentation or omission for an honest services fraud conviction be "material."[37]

Other courts of appeals have yet to directly address, in a post-*Skillin*g, private sector honest services fraud context, whether the government must prove that a defendant intended to cause harm to the victim or that such harm had to be reasonably foreseeable to the defendant. However, based on the pre-*McNally* and pre-*Skilling* case law, courts in the Fourth and the Eleventh Circuit may require "foreseeability of harm" as an element of an honest services fraud prosecution.[38]

Simply, just as there was no uniformity among the courts with respect to elements of honest services fraud prior to *Skilling*, differences in interpreting and applying elements of section 1346 remain even after the decision. Based on court decisions to date, it is reasonable to believe that *Skilling* may not be the last case to address legal issues with regard to section 1346.

---

[35] *Id.* at 983–84 ("Although the schemes in many of our private corruption precedents had a pecuniary impact on the person to whom a fiduciary duty is owed, we have never said that tangible harm is required in such a case."); *see also,* United States v. Tanner, No. 17 CR. 61 (LAP), 2018 WL 1737235, at *6 (S.D.N.Y. Feb. 23, 2018) (discussing whether defendant's actions "benefited or harmed the employer who enjoyed a right to the honest services of its employee, is irrelevant." (citing *Nayak,* 769 F.3d at 981–82)).

[36] United States v. Milovanovic, 678 F.3d 713, 726 (9th Cir. 2012).

[37] *Id.* at 726–27 (citations omitted).

[38] *See, e.g.,* 11th Cir. Pattern Crim. Jury Instr. OI O50.4 (2016) (listing foreseeability of economic harm as an element of honest services fraud based on United States v. deVegter, 198 F.3d 1324, 1329 (11th Cir. 1999)); *see also,* United States v. Lusk, No. 2:15-CR-00124, 2017 WL 508589, at *11 (S.D. W. Va. Feb. 7, 2017) (citing United States v. Vinyard, 266 F.3d 320, 326 (4th Cir. 2001)).

V. Conclusion

To save the honest services statute from a vagueness challenge, the Supreme Court in *Skilling* attempted to limit the reach of section 1346 to those "core" cases involving bribes or kickbacks. The "core" cases were supposed to be the pre-*McNally* honest services fraud cases that had some sort of uniformity and consensus among the various courts. As the section 1346 cases litigated post-*Skilling* demonstrate, however, there are significant questions that remain as to how and when fiduciary duty arises, and whether foreseeable harm to the victim must be shown to prove intent.

Federal prosecutors should be aware of the future litigation risks that the "intangible right to honest services" theory poses prior to pursuing this theory of mail/wire fraud. Practically speaking, the only section 1346 cases post-*Skilling* that should survive any future constitutional vagueness challenge may be those cases where (1) fiduciary duty arises from relationships already well established in the law (categorical approach); (2) the breach of that duty was brought about through a bribe or a kickback; and (3) the victim suffered some type of economic harm, or such harm was foreseeable to the defendant.

About the Author

Byung J. "BJay" Pak was confirmed by the U.S. Senate on September 28, 2017 as the United States Attorney for the Northern District of Georgia. From 2002–2008, he served as an Assistant United States Attorney in the Criminal Division, and was a member of the Narcotics and OCDETF Section, as well as the Economic Crimes Section. Previously, BJay was in private practice handling complex civil litigation, white collar investigation, and prosecution matters. He earned his J.D., summa cum laude, and Order of the Coif, from the University of Illinois College of Law, where he was a Harno Scholar. He also served as the Notes Editor for the Recent Decisions Section of the Illinois Bar Journal. He clerked for the Honorable Richard Mills, United States District Judge for the Central District of Illinois. He received his B.B.A. in accounting from Stetson University in DeLand, FL, and is a registered Certified Public Accountant in the State of Illinois.

Page Intentionally Left Blank

Corporate Accountability for the Opioid Epidemic

Andrew E. Lelling
United States Attorney
District of Massachusetts

I. Introduction

The epidemic of opioid abuse and addiction in the United States is, by now, distressingly familiar. In 2017 alone, over 70,000 people suffered a fatal opioid overdose;[1] countless others suffered nonfatal overdoses and were revived using Narcan.[2] Added to the staggering human cost is the economic burden of chronic opioid use. Princeton economist Alan Krueger suggests that chronic opioid use may account for more than 20% of the decline in American labor force participation from 1999–2015.[3]

To combat this public health crisis, the Department of Justice is dedicating tremendous resources to reduce the supply of illicit opioids (primarily heroin and, increasingly, fentanyl). Wiretaps, undercover investigations, and indictments charging violations of 21 U.S.C. §§ 841 and 846 are the most widely recognized elements of this work.[4] Research has shown, however, that street-level

---

[1] *See* Overdose Death Rates, NAT'L INST. ON DRUG ABUSE, https://www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates (last visited Oct. 8, 2018). This article includes overdose deaths from natural and semi-synthetic opioids, heroin, and synthetic opioids other than methadone, such as fentanyl.

[2] *See* Naloxone for Opioid Overdose: Life-Saving Science, NAT'L INST. ON DRUG ABUSE, https://www.drugabuse.gov/publications/naloxone-opioid-overdose-life-saving-science/naloxone-opioid-overdose-life-saving-science (last visited Oct. 8, 2018).

[3] Fred Dews, *How the Opioid Epidemic has Affected the U.S. Labor Force, County-by-County*, BROOKINGS (Sept. 7, 2017), https://www.brookings.edu/blog/brookings-now/2017/09/07/how-the-opioid-epidemic-has-affected-the-u-s-labor-force-county-by-county/.

[4] *See* 21 U.S.C. § 841 (criminalizing the manufacture, distribution and possession with intent to distribute controlled substances); *see also* 21 U.S.C. § 846 (criminalizing conspiracy to commit the crimes listed in 21 U.S.C. § 841).

distribution of illicit opioids is only one part of the problem. The United States Center for Disease Control estimates that *nearly half* of all opioid overdose deaths involve a prescription opioid.[5] Studies have found that 80% of heroin users previously used prescription opioids,[6] and many opioid addicts first used these drugs pursuant to a legitimate medical prescription.[7] Moreover, about 25% of all patients prescribed opioids for chronic pain eventually misuse their prescriptions, and about 10% of all such patients develop an opioid use disorder.[8] The economic burden of this misuse in the United States is $78.5 billion a year, including the costs of healthcare, lost productivity, addiction treatment, and criminal justice involvement.[9]

Because prescription opioids function as a primary path to opioid addiction and because of the personal, societal, and economic consequences that flow from that addiction, investigating and prosecuting illegal distribution of prescription opioids is a necessary adjunct to more traditional forms of enforcement. Recognizing this, the Department of Justice aggressively pursues criminal and civil

---

[5] *See Opioid Overdose*, CTR. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/drugoverdose (last visited Oct. 8, 2018).

[6] *See* Opioid Overdose Crisis, NAT'L INST. ON DRUG ABUSE, https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis (last visited Oct. 8, 2018); *see also* PRADIP K. MUHURI ET AL., SAMHSA CTR. FOR BEHAVIORAL HEALTH STATISTICS AND QUALITY DATA REVIEW, ASSOCIATIONS OF NONMEDICAL PAIN RELIEVER USE AND INITIATION OF HEROIN USE IN THE UNITED STATES (2013).

[7] *See also* Robert G. Carlson et al., *Predictors of Transition to Heroin Use Among Initially Non-Opioid Dependent Illicit Pharmaceutical Opioid Users: A Natural History Study*, 160 DRUG AND ALCOHOL DEPENDENCE 127; *see also* Ameet Sarpatwari et al., *The Opioid Epidemic: Fixing a Broken Pharmaceutical Market*, 11 HARV. L. & POL'Y REV. 463 (2017). "A fundamental cause of the epidemic was—and continues to be—an over-prescription of opioids. From 2000 to 2010, the number of prescriptions for oral opioid analgesics rose 104%." *Id.* at 464; *see also* Brian D. Sites et al., *Increases in the Use of Prescription Opioid Analgesics and the Lack of Improvement in Disability Metrics Among Users,* 39 REGIONAL ANESTHESIA & PAIN MED. 6 (2014).

[8] *See* Opioid Overdose Crisis, NAT'L INST. ON DRUG ABUSE, https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis (last visited Oct. 8, 2018).

[9] *Id.*

charges against corporate opioid manufacturers and distributors, including individual executives and employees.

II. Criminal and civil prosecutions involving manufacturers and distributors of prescription opioids

In his 1995 Presidential Address to the American Pain Society, Dr. James Campbell first presented the idea of evaluating pain as a fifth "vital sign."[10] Campbell's idea caught on nationally, prompting healthcare providers to separately assess pain, often using a "pain scale."[11] In response to the newfound emphasis on pain treatment, clinicians began prescribing more opioids.[12] Pharmaceutical companies played an active role in this trend by reassuring the medical community that there was no significant risk of addiction from use of prescription opioids to treat pain, even chronic, long term pain.[13] The available data, however, strongly suggests otherwise.[14]

A. Theories of criminal and civil liability

The government has successfully prosecuted pharmaceutical manufacturers and distributors under a variety of civil and criminal statutes. To date, the most common theories of criminal and civil liability are:

- *Anti-Kickback Statute*, 42 U.S.C. § 1320a-7b: The Anti-Kickback Statute prohibits knowingly and willfully offering, paying, soliciting, or receiving remuneration intended to induce submission of a claim to a federal healthcare program. For example, the Anti-Kickback Statute would prohibit an opioid manufacturer from using expensive meals or travel to induce a physician to prescribe the manufacturer's drug for Medicare patients. Notably, a claim resulting from a violation of the

[10] Natalie E. Morone & Deborah K. Weiner, *Pain as the Fifth Vital Sign: Exposing the Vital Need for Pain Education*, 35 CLINICAL THERAPEUTICS 1728 (2013).
[11] *See Id*.
[12] *See Id*.
[13] *See* Ty E. Howard & Scarlett Singleton Nokes, '*Opioids and Legal Enforcement—A Primer*,' in HARRISMARTIN'S DRUGS & MEDICAL DEVICES, BRADLEY (Jul. 2018).
[14] *See supra* notes 1–2 & 5–8.

Anti-Kickback Statute is a false or fraudulent claim for purposes of the False Claims Act (described below).[15]

- *Food, Drug, and Cosmetic Act (FDCA)*, 21 U.S.C. § 331: The FDCA prohibits: (1) the introduction of misbranded or adulterated drugs into interstate commerce (21 U.S.C. § 331(a)); (2) the introduction of an unapproved new drug into interstate commerce (21 U.S.C. § 331(d)); and (3) the failure to establish or maintain certain records or make certain reports or permit access to certain records or reports (21 U.S.C. § 331(e)). For instance, the FDCA would prohibit an opioid manufacturer from improperly marketing a drug by falsely claiming that it had certain benefits over another drug when, in fact, it did not. Under the FDCA, the same prohibited acts may give rise to civil and criminal liability.[16] The FDCA creates two tiers of criminal offenses for the interstate shipment of unapproved, adulterated or misbranded drugs: (1) strict liability misdemeanor offenses; and (2) felony offenses for acts done with an intent to defraud or mislead.[17]
- *False Claims Act*, 31 U.S.C. § 3729–33: The False Claims Act imposes civil liability on any person who knowingly presents, or causes to be presented, a false or fraudulent claim to the United States government.[18] For example, if an opioid manufacturer violated the Anti-Kickback Statute by providing a physician with an expensive meal or travel, the manufacturer would face liability under the False Claims Act for the claims to Medicare that resulted from physician's subsequent prescribing of the manufacturer's drug.
- *Controlled Substances Act (CSA)*, 21 U.S.C. §§ 801–904 (and corresponding federal regulations): Among other things, the CSA prohibits any manufacturer, distributor, or dispenser from distributing or dispensing a controlled substance without a valid prescription.[19] The prescription "must be issued for a legitimate medical purpose by an individual practitioner acting in the usual course of his professional practice. The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner, but a corresponding responsibility rests with the pharmacist who fills the

[15] *See* 42 U.S.C. § 1320a–7b(g).
[16] *See* 21 U.S.C. § 332 (civil action); 21 U.S.C. § 333(a) (criminal liability); 21 U.S.C. § 334 (seizures).
[17] 21 U.S.C. §§ 333(a)(1), (2).
[18] 31 U.S.C. § 3729(a)(1)(A).
[19] 21 U.S.C. § 842(a)(1).

prescription."[20] For example, a pharmacy would face liability under the CSA if it dispensed opioids to an individual who had presented a prescription that the pharmacy had reason to believe was fraudulent.

The CSA makes it unlawful "to refuse or negligently fail to make, keep or furnish any record, report, notification, declaration, or order form, statement, invoice, or information required under" any provision of the CSA.[21]

The CSA also requires that manufacturers and distributors maintain certain records including: (1) an accurate record of each controlled substance "manufactured, received, sold, delivered or otherwise disposed of;"[22] (2) an inventory at the time the person begins dispensing controlled substances and every two years thereafter;[23] and (3) prescriptions of controlled substances dispensed.[24]

The CSA further requires manufacturers and distributors to furnish the following records to the Drug Enforcement Administration (DEA): (1) reports of a theft or significant loss of controlled substances, 21 C.F.R. § 1301.74(c); and (2) reports concerning a suspicious order of controlled substances, that is, an order which is of "unusual size," which "deviat[es] substantially from a normal pattern," or which is "of unusual frequency."[25] For example, a hospital would face liability under the CSA if it discovered that a nurse had stolen hundreds of OxyContin tablets and then failed promptly to report the theft to the DEA. Likewise, the hospital would face liability if its records did not account for the dispensing of all OxyContin tablets the hospital had purchased. An opioid manufacturer would face liability where it distributed hundreds of thousands of pills to a small pharmacy servicing a small population and failed to detect and report that "suspicious order" to the DEA.[26]

---

[20] 21 C.F.R. § 1306.04(a).

[21] § 842(a)(5).

[22] 21 U.S.C. § 827(a)(3); 21 C.F.R. §§ 1304.21, 1304.22.

[23] 21 U.S.C. § 827(a); 21 C.F.R. § 1304.11.

[24] 21 C.F.R. § 1304.04(h)(2), (4).

[25] 21 C.F.R. § 1301.74(b).

[26] Press Release, U.S. Dep't of Justice, Department of Justice Announces Regulatory Steps to Address Opioid Epidemic (July 11, 2018). On July 11, 2018, the Department of Justice finalized a new policy for the DEA whereby the Attorney General, through the DEA, can set aggregate production quotas

- *Racketeer Influenced and Corrupt Organizations Act (RICO)*, 18 U.S.C. § 1961, *et seq.*:[27] Generally, RICO prohibits a person associated with an enterprise to conduct or participate in the conduct of the enterprise through a pattern of racketeering activity.[28] An enterprise can include any partnership, corporation, association or other legal entity, or group of individuals associated in fact.[29] Racketeering activity can include conduct punishable under the CSA, as well as mail and wire fraud, among other things.[30]

B. Cases against pharmaceutical manufacturers

The following cases illustrate the Department of Justice's commitment to combatting the opioid epidemic through the prosecution of pharmaceutical manufacturers.

1. Insys Therapeutics, Inc.

Insys Therapeutics, Inc. is an Arizona-based pharmaceutical corporation that, in March 2012, began marketing a powerful, fentanyl-based pain medication called "Subsys." In October 2017, a federal grand jury in Massachusetts returned an indictment charging seven former Insys executives with offenses relating to the sale of Subsys. Those indicted included the company's founder and owner, the former CEO and President, the former Vice President of Sales, the former National Director of Sales, former Regional Sales Directors, and the former Vice President of Managed Markets. The indictment charged each of these executives with conspiring to commit racketeering offenses (18 U.S.C. § 1962(d)), conspiring to commit mail fraud and wire fraud (18 U.S.C. § 1349), and conspiring to provide kickbacks and bribes (18 U.S.C. § 371, 42 U.S.C. § 1320a-7b(b)(2)).

---

for Schedule I and II controlled substances including manufacturing and procurement quotas for manufacturers. *Id.* This will give the DEA the ability to limit the volume of prescription opioids produced by any given manufacturer.

[27] Until the *Insys* case, described herein, the government had not prosecuted a pharmaceutical company using RICO.

[28] 18 U.S.C. § 1962(c).

[29] 18 U.S.C. § 1961(4).

[30] *See* 18 U.S.C. §§ 1341, 1343. The government also has used the traditional mail and wire fraud statutes to prosecute pharmaceutical companies and/or distributors where the company's executives and employees have engaged in a scheme to defraud (e.g., by making false representations) for the purpose of obtaining money and property, often in the form of additional opioid sales.

Broadly, the indictment alleges that:

(1) The defendants paid kickbacks and bribes to medical practitioners in order to cause those practitioners to write more prescriptions for Subsys, and to write prescriptions at higher doses. The bribes and kickbacks took various forms, including speaker fees and honoraria for marketing events, administrative support for practitioners, and fees paid to pharmacies affiliated with practitioners;
(2) The defendants sought to mislead and defraud insurance companies (and their agents) into authorizing payment for Subsys, an expensive drug. The indictment alleges that the defendants knew that insurers would likely authorize payment for Subsys only in limited circumstances—the drug was FDA approved only to manage breakthrough pain in cancer patients for whom other opioid treatments were no longer effective. Accordingly, Insys employees, working from a call center at the company's headquarters, defrauded insurers by suggesting that they worked for the prescribing practitioners, and then lying about patient diagnoses, the type of pain being treated, and the patient's course of treatment with other medications, in order to convince insurers and their agents to pay for Subsys and increase profits at Insys;
(3) By bribing practitioners to prescribe Subsys outside the usual course of professional practice, and by defrauding insurers, the defendants sought to cause the illicit distribution and sale of Subsys, which, as a fentanyl-based opioid, is a Schedule II controlled substance and is tightly regulated under the CSA; and
(4) When wholesalers of Subsys raised concerns about the volume of fentanyl purchased by certain pharmacies, the defendants eliminated those wholesalers from the chain of distribution by shipping directly to the pharmacies, partly in an effort to avoid DEA scrutiny.[31]

The case is now pending in federal district court in Boston.[32]

[31] *See* First Superseding Indictment, United States v. Babich, et al., No. 16-cr-10343-ADB (D. Mass. Oct. 24, 2017), ECF No. 183-2.
[32] Several criminal cases against practitioners who participated in this scheme have been charged in other districts across the country.

2. Purdue Frederick Company, Inc.

The Purdue Frederick Company, Inc. ("Purdue") introduced the drug OxyContin in 1996.[33] Thereafter, according to the government allegations, Purdue and its top executives launched an aggressive marketing campaign claiming that OxyContin was a miracle drug—one that provided long acting pain relief *with little risk of addiction or abuse*.[34] As a result, Purdue earned approximately $2.8 billion in revenue from the sale of OxyContin between January 1996 and June 30, 2001.[35] But as Purdue and its executives knew, OxyContin was highly addictive.[36] Accordingly, on May 10, 2007, the United States Attorney's Office for the Western District of Virginia charged Purdue, its President and CEO, its Chief Legal Officer, and its Chief Scientific Officer by criminal information, with introduction of a misbranded drug into interstate commerce, in violation of 21 U.S.C. §§ 331(a), 352(a), and 333(a)(2).[37] Specifically,

---

[33] *See* U.S. GEN. ACCOUNTING OFFICE, PRESCRIPTION DRUGS: OXYCONTIN ABUSE AND DIVERSION AND EFFORTS TO ADDRESS THE PROBLEM (2003). OxyContin is a controlled substance that contains the opioid oxycodone.

[34] News Release, U.S. Attorney's Office, W.D. of Va., The Purdue Frederick Company, Inc. and Top Executives Plead Guilty to Misbranding Oxycontin; Will Pay Over $600 Million (May 10, 2007).

[35] *See* Exhibit B to Information, Agreed Statement of Facts, United States v. The Purdue Frederick Co., Inc. et al., No. 07-00029-JPJ, ECF No. 5-2 (W.D. Va. May 10, 2007).

[36] *See id.*

[37] News Release, U.S. Attorney's Office, W.D. of Va., The Purdue Frederick Company, Inc. and Top Executives Plead Guilty to Misbranding Oxycontin; Will Pay Over $600 Million (May 10, 2007). The company was charged with felony misbranding, that is, misbranding with the intent to defraud or mislead, while the individual defendants were charged with misdemeanor misbranding, a strict liability offense based on the executives' positions as responsible corporate officers. *Id.; see also* 21 U.S.C. § 331(a); *see* United States v. Park, 421 U.S. 658, 673 (1975) (explaining that "Congress has seen fit to enforce the accountability of responsible corporate agents dealing with products which may affect the health of consumers by penal sanctions cast in rigorous terms"); *see* United States v. Dotterweich, 320 U.S. 277, 281 (1943) (explaining that FDCA is one of those statutes that "[i]n the interest of the larger good . . . puts the burden of acting at hazard upon a person otherwise innocent but standing in responsible relation to a public danger."); *see also* United States v. Wiesenfeld Warehouse Co., 376 U.S. 86, 91 (1964) (explaining that "[i]t is settled law in the area of food and drug

the Information alleged that, from December 1995 until June 2001, Purdue supervisors and employees marketed and promoted OxyContin as "less addictive, less subject to abuse and diversion, and less likely to cause tolerance to withdrawal than other pain medications."[38] For instance, the Information alleged that Purdue sales representatives told healthcare providers that "OxyContin potentially creates less chance for addiction than other opioids," "that patients could stop [taking OxyContin] abruptly without experiencing withdrawal symptoms and that patients who took OxyContin would not develop tolerance to the drug."[39] On May 10, 2007, Purdue and its three top executives pled guilty to both counts of the Information.[40] Pursuant to its plea agreement with the United States, Purdue agreed to pay monetary sanctions of $600 million—reportedly the largest penalty in the history of the pharmaceutical industry at that time, while the three corporate executives agreed to pay an additional $34.5 million.[41]

Purdue also entered into a corresponding civil settlement with the United States.[42] As part of that civil settlement, Purdue was excluded from participation in federal healthcare programs for 25 years.[43] In February 2018, Purdue laid off much of its sales force and announced it would no longer promote opioids to doctors. In June 2018, Purdue laid off additional sales representatives and announced that its remaining sales force would focus on promoting non-opioid products.[44]

---

regulation that a guilty intent is not always a prerequisite to the imposition of criminal sanctions.").

[38] United States v. Purdue Frederick Co. Inc., 495 F. Supp. 2d 569, 571 (W.D. Va. 2007) (quoting the Information).

[39] *Id.*

[40] *See* News Release, *supra* note 34.

[41] *Purdue Frederick Co. Inc.*, 495 F. Supp. 2d at 572–73.

[42] *See id.* at 572.

[43] *See id.*

[44] Nate Raymond, OxyContin Maker Purdue Pharma Cuts Remaining Sales Force, REUTERS BUSINESS NEWS (June 20, 2018), https://www.reuters.com/article/us-usa-opioids-purduepharma/oxycontin-maker-purdue-pharma-cuts-remaining-sales-force-idUSKBN1JG1W6.

3. Galena Biopharma Inc.

Galena Biopharma, Inc. (Galena)[45] was a pharmaceutical company founded in Worcester, Massachusetts, but based in California.[46] In September 2017, Galena paid $7.55 million to resolve federal civil False Claims Act allegations. In particular, the government alleged that Galena paid kickbacks to doctors to induce them to prescribe Abstral, a highly addictive fentanyl-based opioid. According to the government, Galena offered multiple types of kickbacks including: (1) free meals; (2) thousands of dollars to attend an advisory board meeting that was planned and attended by Galena sales team members; (3) tens of thousands of dollars to enter into a performance-based rebate agreement with a physician-owned pharmacy; and (4) payment in exchange for patient referrals to a patient registry study.[47] Separately, two of the physicians who received remuneration from Galena were tried, convicted, and sentenced to prison in the United States District Court for the Southern District of Alabama for, among other things, offenses relating to their prescriptions for Abstral.[48]

4. Mallinckrodt LLC

Mallinckrodt LLC was once one of the largest manufacturers of generic oxycodone. In July 2017, the company agreed to pay a record $35 million to resolve allegations that it violated civil provisions of the CSA. Specifically, the government alleged that, from 2008–2011, Mallinckrodt filled suspiciously large oxycodone orders, but failed to detect them or to notify the DEA. The government also alleged that Mallinckrodt violated DEA recordkeeping requirements by failing to

---

[45] Press Release, SELLAS Life Sciences Group, SELLAS Life Sciences Group Successfully Completes Business Combination with Galena Biopharma (Dec. 29, 2017).

[46] *See* Galena Biopharma Inc. (GALE) Plunges 5.11% on January 01, EQUITIES.COM (Jan. 1, 2018), https://www.equities.com/news/galena-biopharma-inc-gale-plunges-5-11-on-january-01.

[47] Press Release, U.S. Dep't. of Justice, Galena Biopharma Inc. to Pay More Than $7.55 Million to Resolve Alleged False Claims Related to Opioid Drug (Sept. 8, 2017).

[48] *Id*.

keep track of the number of oxycodone tablets it was manufacturing.[49] Apart from the significant monetary penalty, Mallinckrodt also entered into an agreement with the DEA whereby the company agreed to, among other things, analyze and report data it collects from customer orders in an effort to identify suspicious sales.[50]

C. Cases against pharmaceutical distributors

The following cases illustrate the government's success in obtaining civil and criminal settlement agreements from pharmaceutical distributors, including wholesalers, hospitals and pharmacies—each of which plays a key role in ensuring that opioids are disbursed to patients only through legitimate prescriptions for a proper medical purpose.

1. Wholesalers

McKesson Corporation

McKesson Corporation is a wholesale distributor of pharmaceuticals, including opioids. In or about 2007, the government claimed that McKesson failed to report suspicious orders of controlled substances from some of its customers. As a result, in May 2008, McKesson entered into a settlement with the United States requiring the company to pay a $13.25 million penalty. McKesson was also required to develop a controlled substance monitoring program and report any future suspicious orders.

From 2009 through January 2017, McKesson violated its own controlled substance monitoring program (as well as the CSA and the corresponding federal regulations) by, among other things, failing to conduct adequate due diligence of its customers, failing to keep complete and accurate records for many of its customers, and bypassing suspicious order reporting procedures. As a result, the Department of Justice forced McKesson to pay an additional $150 million to resolve these claims. As part of its settlement agreement with the government, McKesson acknowledged that it failed to report certain orders that it should have deemed suspicious.[51]

---

[49] Press Release, U.S. Dep't. of Justice, Mallinckrodt Agrees to Pay Record $35 Million Settlement for Failure to Report Suspicious Orders of Pharmaceutical Drugs and for Recordkeeping Violations (July 11, 2017).
[50] *See* Memorandum of Mallinckrodt Administrative Agreement (July 7, 2017).
[51] *See* McKesson Settlement Agreement and Release (Jan. 5, 2017).

Cardinal Health, Inc.

Like McKesson, Cardinal Health, Inc. (Cardinal) is a wholesale distributor of pharmaceuticals. In 2008, Cardinal entered into a Memorandum of Agreement (MOA) with the DEA to resolve claims that one of its distribution facilities disbursed suspiciously large quantities of hydrocodone, a synthetic opioid. Pursuant to that agreement, Cardinal paid a $34 million penalty.[52] In 2012, Cardinal entered into a second MOA with the DEA after violating the terms of its 2008 MOA by failing to maintain effective controls against the diversion of controlled substances and failing to detect and report suspicious orders of controlled substances.[53] Pursuant to the 2012 MOA, Cardinal agreed to take steps to correct these failures.[54] The third time is not always the charm. In December 2016, the United States again alleged that Cardinal had violated the CSA in multiple states by "failing to report suspicious orders of controlled substances to pharmacies located in those states."[55] Cardinal paid a $44 million penalty to resolve those claims with the government.[56]

2. Hospitals and Health Networks

Effingham Health System

Effingham Health System ("Effingham"), located in Georgia, includes Effingham Hospital and numerous other healthcare treatment facilities. In 2017, the DEA began investigating Effingham after receiving reports of drug diversion. The investigation revealed that, from about 2013 through 2017, tens of thousands of oxycodone 30 mg tablets were unaccounted for and likely diverted from Effingham, violating Effingham's obligations under the CSA to provide effective controls to guard against theft and loss of controlled

---

[52] *See* Cardinal Health Reaches Settlement with DEA, HALL RENDER (May 16, 2012), http://www.hallrender.com/2012/05/16/cardinal-health-reaches-settlement-with-dea/; *see also* Memorandum of Cardinal Health Administrative Agreement (May 14, 2012).
[53] *See* Memorandum of Cardinal Health Administrative Agreement (May 14, 2012).
[54] *See id*.
[55] Press Release, U.S. Dep't. of Justice, Cardinal Health Agrees to $44 Million Settlement for Alleged Violations of Controlled Substances Act (Dec. 23, 2016).
[56] *Id.*

substances. The DEA also found that Effingham failed to notify the DEA of the suspected diversion. As a result of the DEA's investigation, Effingham agreed to pay the United States $4.1 million—the nation's largest hospital drug diversion civil penalty in United States history. Effingham reportedly cooperated with the DEA in its investigation and entered into an agreement to memorialize a plan to address its deficiencies and "avoid diversions in the future."[57]

Massachusetts General Hospital

In 2013, the DEA launched an investigation into drug diversion at Massachusetts General Hospital (MGH), the largest hospital in Massachusetts,[58] after MGH disclosed that two of its nurses stole nearly 16,000 pills—mostly oxycodone—from the hospital.[59] The nurses stole the drugs from "automated dispensing machines that MGH used to store and dispense prescription medications."[60] A subsequent DEA audit revealed that over 20,000 pills were unaccounted for, medication inventories were missing or incomplete, and hundreds of drug records were missing, all in violation of MGH's responsibilities under the CSA.[61] MGH cooperated with the DEA's investigation and disclosed additional violations of the CSA including, for instance: that a pediatric nurse with a twelve year substance abuse problem had injected himself with Dilaudid (a type of synthetic opioid) while at work, a doctor had prescribed controlled substances to his patients without seeing them or maintaining medical records, nurses were able to divert prescription drugs for years without detection, and medical staff failed to properly secure controlled substances, even, on occasion, bringing the drugs to lunch.[62]

As a result of the DEA's investigation, in September 2015, MGH agreed to pay the United States $2.3 million and to enter into a three

---

[57] Press Release, U.S. Dep't. of Justice, Southern District of Georgia Announces Largest Hospital Drug Diversion Civil Penalty Settlement in U.S. History (May 16, 2018).

[58] *See* MGH Settlement Agreement 1 (Sept. 28, 2015).

[59] Press Release, U.S. Dep't. of Justice, MGH to pay $2.3 Million to Resolve Drug Diversion Allegations (Sept. 28, 2015).

[60] *Id.*

[61] *Id.; see also* MGH Settlement Agreement 1–2 (Sept. 28, 2015).

[62] Press Release, U.S. Dep't. of Justice, MGH to Pay $2.3 Million to Resolve Drug Diversion Allegations (Sept. 28, 2015); *see also* MGH Settlement Agreement, Attachment 2, 8–11 (Sept. 28, 2015).

year corrective plan requiring MGH to implement diversion controls, employ a full time Drug Diversion Compliance Officer, establish a drug diversion team, conduct mandatory annual training for all staff with authorized access to controlled substances, and hire external auditors to conduct unannounced audits at all MGH facilities.[63]

Dignity Health

In late 2010 and 2011, the DEA began an investigation of Dignity Health (Dignity)—California's largest hospital provider and the country's fifth largest health system—following reported losses of over 20,000 hydrocodone tablets from an outpatient pharmacy affiliated with Dignity.[64] A subsequent DEA audit revealed shortages of a number of controlled substances, including hydrocodone.[65] The DEA's investigation further revealed that several Dignity locations violated the CSA by "failing to keep accurate records [. . .] designed to prevent drug diversion."[66] In July 2014, Dignity "agreed to pay the United States $1.55 million to settle claims of deficiencies [in] the handling of controlled substances at its hospitals and clinics" in violation of the CSA.[67] In conjunction with the monetary settlement, Dignity agreed to an extensive compliance regime including annual external audits, restricted access to areas containing controlled substances, and increased physical counts and inventories of controlled substances.[68]

Intermountain Healthcare

According to the government, from September 2007 through March 2015, a former medical assistant who worked at a clinic near Ogden, Utah, used a doctor's DEA registration number to write 244 prescriptions of Oxycodone 30 mg tablets (46,616 pills) and another 151 prescriptions for controlled substances, for herself and two family members.[69] A pharmacy, also located near Ogden, filled

---

[63] *See* MGH Settlement Agreement, Attachment 3, 8–11 (Sept. 28, 2015).
[64] Press Release, U.S. Dep't. of Justice, Dignity Health Agrees to Pay $1.55 Million in Civil Penalties to Resolve Controlled Substances Act Claims (July 16, 2014).
[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] *See id*.
[69] Press Release, U.S. Dep't. of Justice, Settlement Reached in Significant Drug Diversion Case (Dec. 8, 2017).

each of the prescriptions, and the former medical assistant picked them up. Both the clinic and pharmacy were affiliated with Intermountain Healthcare.[70] In December 2017, "Intermountain . . . agreed to pay the United States $1 million to resolve allegations that lax controls enabled a former employee to divert [prescriptions drugs] for personal use."[71]

3. Pharmacies

CVS Pharmacy, Inc.

After receiving an increased number of calls regarding forged oxycodone prescriptions at CVS pharmacies, the DEA initiated multiple investigations into CVS Pharmacy, Inc. (CVS).[72] The first investigation revealed 403 forged prescriptions filled at 40 CVS stores in Massachusetts and New Hampshire.[73] The second investigation revealed 120 forged prescriptions filled at ten CVS stores in and around Boston, Massachusetts.[74] "The DEA estimated the street value of the diverted [oxycodone] pills to be over $1 million."[75] Interestingly, the forged prescriptions were traced to just a handful of individuals. By way of example, one of the forgers was banned in 2011 from filling prescriptions at CVS.[76] Nonetheless, she was able to fill 56 fake oxycodone prescriptions (purportedly signed by a dentist) at five CVS locations by opening a new patient profile using a different last name (but her actual driver's license number).[77] Another forger signed a dentist's name on 131 hydrocodone prescriptions and filled them at eight CVS stores. One store filled 29 forged prescriptions for the forger in just six months.[78]

Under the CSA, pharmacies have a responsibility to ensure they fill only valid prescriptions issued for a legitimate medical purpose. Here, the government alleged that CVS ignored red flags that would have uncovered the fraud. As a result, in June 2016 CVS agreed to

---

[70] *See id*.
[71] *Id*.
[72] Press Release, U.S. Dept. of Justice, CVS to Pay $3.5 Million to Resolve Allegations that Pharmacists Filled Fake Prescriptions (June 30, 2016).
[73] *Id*.
[74] *Id*.
[75] *Id*.
[76] *Id*.
[77] *Id*.
[78] *Id*.

pay $3.5 million to the United States and entered into a three year compliance agreement with the DEA requiring the company to maintain and enhance programs for detecting and preventing diversion of controlled substances.[79]

Rite Aid Corporation

A federal criminal investigation in the Southern District of West Virginia revealed that, between January 2009 and October 2012, Rite Aid Corporation improperly sold pseudoephedrine (PSE), a methamphetamine precursor.[80] In particular, Rite Aid's training and corporate procedures led employees to believe that they could only deny the sale of PSE to a customer if the sale exceeded a PSE purchase limit and not, for instance, if the employee suspected the customer wanted the PSE for an improper purpose, that is, to manufacture methamphetamine.[81] In order to resolve this criminal investigation, Rite Aid agreed to pay $4 million (80% of Rite Aid's gross profits from the sale of PSE in West Virginia during the relevant timeframe).[82] In addition, Rite Aid accepted responsibility for its improper sales practices, and agreed to take remedial measures regarding its sales of PSE including, for instance, requiring that PSE products be placed out of view of customers, requiring pharmacists to provide counseling for customers seeking to purchase PSE, and training its staff to identify customers who may be purchasing PSE for the manufacture of methamphetamine.[83] While this case did not involve opioids, the same theories of liability would apply to a case involving, for instance, prescriptions for oxycodone.

Costco Pharmacy

From January 2012 through December 2015, Costco Pharmacy dispensed controlled substances in a manner that violated the CSA. These violations included: filling prescriptions from practitioners who did not have a valid DEA registration number; incorrectly recording

---

[79] *Id*.
[80] *See* Press Release, U.S. Dep't of Justice, U.S. Attorney's Office Enters Settlement with Rite Aid Based on Improper Sales of Meth Precursor Pseudoephedrine, Rite Aid Settlement Fact Sheet Attachment (Jan. 24, 2018).
[81] *Id*.
[82] *Id*.
[83] *Id*.

the practitioner's DEA number; filling prescriptions outside the scope of the practitioner's DEA registration; filling prescriptions that did not contain all required information; and other record-keeping violations.[84] As a result, in January 2017, Costco agreed to pay $11.75 million to the United States and take remedial measures, for example, by purchasing a new pharmacy management system and implementing an audit program of its pharmacy locations.[85] In addition, under the terms of the settlement, the DEA may "conduct unannounced and unrestricted inspections of all DEA registered Costco Pharmacy locations" for a period of three years.[86]

Safeway

In April 2014, the DEA began an investigation into Safeway pharmacies after learning that certain pharmacies in Washington and Alaska did not timely notify the DEA after learning that employees stole tens of thousands of hydrocodone tablets.[87] The investigation later revealed that such failure to report was a widespread practice of Safeway pharmacies between 2009 and 2014.[88] As a result of the investigation, in July 2018, Safeway agreed to pay $3 million to the United States and "implement a compliance agreement with the [DEA] to ensure such notification lapses do not happen again."[89]

III. Conclusion

We cannot successfully reduce the supply of illicit opioids by focusing only on street level distribution. We must, in addition, target otherwise legitimate corporate manufacturers and distributors of prescription opioids when lax controls and other practices lead to legally manufactured opioids being made available for illegal use. Criminal and civil enforcement, as summarized above, can effectively deter businesses from failing to invest in the internal processes and

[84] Press Release, U.S. Dep't. of Justice, Costco Wholesale to Pay $11.75 Million to Settle Allegations of Lax Pharmacy Controls (Jan. 19, 2017).
[85] *Id.*
[86] *Id.*
[87] Press Release, U.S. Dep't of Justice, Safeway Pharmacies Pay $3 Million to Resolve Allegations Chain Failed to Timely Report Drug Diversion (July 18, 2017).
[88] *Id.*
[89] *Id.*

training necessary to keep their opioids from being distributed for illicit purposes.[90]

About the Author

Andrew E. Lelling is the United States Attorney for the District of Massachusetts. Before his appointment, Andrew Lelling was a federal prosecutor for over 15 years, serving first in the Civil Rights Division at the Justice Department and later at the United States Attorney's Offices for the Eastern District of Virginia and the District of Massachusetts. Before serving as a federal prosecutor, Mr. Lelling was Counsel to the Assistant Attorney General for the Civil Rights Division, focusing on criminal civil rights enforcement, voting rights enforcement actions, and civil investigations of major city police departments.

Before joining the Justice Department, Mr. Lelling was a senior litigation associate at Goodwin Procter in Boston and a litigation associate at LeBoeuf, Lamb, Greene & MacRae in New York. He also clerked for the U.S. District Court Chief Judge B. Avant Edenfield in the Southern District of Georgia. Mr. Lelling graduated cum laude from University of Pennsylvania Law School in 1994 and received a Bachelor of Arts in Literature & Rhetoric from Binghamton University in 1991. He is a member of the Federalist Society and a former member of the Boston Bar Journal's Board of Editors.

[90] Press Release, U.S. Dep't of Justice, Attorney General Sessions Announces New Prescription Interdiction & Litigation Task Force (Feb. 27, 2018). In February 2018, the Department of Justice announced the creation of the Department of Justice Prescription Interdiction & Litigation Task Force (PIL). PIL's mission is to "aggressively deploy and coordinate all available criminal and civil law enforcement tools to reverse the tide of opioid overdoses in the United States, with a particular focus on opioid manufacturers and distributors."

Note from the Editor-in-Chief

This issue marks a milestone here at the Publications Unit. The Deputy Attorney General announced that the name of the United States Attorneys' Bulletin is changed to the Department of Justice Journal of Federal Law and Practice beginning with this issue. The Bulletin was first published in 1953 and has served the United States Attorney community and Department family well since then.

Two years ago, EOUSA's Office of Legal Education under the leadership of Cammy Chandler set a goal of making the Bulletin one of the most respected journals in the nation and the premier law journal on federal practice. We have come a long way toward meeting that goal. Today, it looks and reads like a top quality law journal. OLE adopted the layout, fonts, and style of the top national law journals. The editors closely adhere to the Bluebook® for citation form and the leading law journal style manuals for writing style. We have substantially increased the amount and levels of editing so that today the technical and substantive editing is extensive and comprehensive. The result is a publication the reader can trust.

Beginning in early 2017, the Publications staff developed a close relationship with ODAG. ODAG not only works with the Publications staff to select topics but ODAG attorneys also serve as Points of Contact and recruit authors from inside and outside of the Department to write articles. Consequently, the issues are relevant and timely. During that time, we have published several issues concerning the Attorney General's top priorities, such as violent crime, immigration and human trafficking. With all of those changes, the title Bulletin no longer captured the true nature of the publication. The title Department of Justice Journal of Federal Law and Practice does.

First we want to thank our Director at EOUSA, James A. Crowell, IV and Deputy Director, Suzanne L. Bell, for all their direction and support which made this change possible. We would also like to thank Andrew Goldsmith (ODAG) for his leadership during this transition. Andrew has been instrumental in selecting issue topics and recruiting experienced and talented ODAG attorneys to serve as Points of Contact for our issues. We would like to thank the team here at Publications who put in the long hours and hard work necessary over the last two years to make these changes—Jim Donovan, our prior Bulletin Editor-in-Chief, Ed Hagen, the past USABook Editor, and

Chris Fisanick, the present DOJBook Editor; Associate Editors past and present—Becky Catoe-Aikey, Bren Mercer, Nikki Piquette, Sarah Nielsen, and Gurbani Saini; and University of South Carolina (USC) law clerks past and present—Sarah Tate Chambers, Emily Godwin, Brandy Sanderlin, Joseph Giordano, Joseph Garfunkel, Emily Lary, Carson Sadro, and Aimee Intagliata. We would also like to thank Rosie Taylor. Rosie supervises all of the USC staff here at Publications and is also an editor extraordinaire. We want to thank Shelburne McGovern, the creative artist with Justice Television Network (JTN) who designed all of our cover and front page graphics, and Angela Chase whose team designed and implemented our new SharePoint editing system. Their hard work and dedication has made this change possible.

The ODAG Point of Contact for this issue, Corporate Crime, is Associate Deputy Attorney General Matthew Baughman. He did an excellent job of designing the focus of the issue and recruiting the authors to write for us. He was also instrumental in the review and editing process.

A sincere thank you to all of the above.

Thank you,

K. Tate Chambers