White-Collar Crime

The **Psychology** of White-Collar Crime, And **Why It Matters**

© SHUTTERSTOCK

BY NICOLAS BOURTIN

Anyone who reads the newspapers or listens to our public officials knows two things about white-collar crime: First, white-collar criminals are just like street criminals. They may wear nicer suits and commit their crimes in boardrooms instead of alleyways, but their motivation is the same: greed. And second, white-collar offenders are highly rational. The way to deter their conduct is to ensure that the risks and consequences of being caught outweigh the rewards. As former U.S. Attorney Preet Bharara said in 2012, white-collar criminals "are highly skilled at cost-benefit analysis" and "weigh the risk of getting caught against the potential reward, and they decide it's worth the risk." Stewart, James. "In a New Era of Insider Trading, It's Risk vs. Reward Squared." New York Times, Dec. 7, 2012.

Our criminal justice system continues to evolve around those received truths. In response to every financial crisis—from the S&L scandal of the late 1980s, to Enron and accounting fraud cases of the early 2000s, to the financial crisis of 2008-09—Congress has enacted ever stricter laws to combat and punish white-collar criminals, and federal and state law enforcement agencies have poured ever more resources into investigating and prosecuting white-collar crime. And investigative techniques once reserved for organized crime and drug cartels, such as wiretaps, undercover agents, and informants, have in recent years been used to great effect against white-collar criminals.

The psychology of white-collar crime is different from street crime; and white-collar defendants typically do not weigh risk and reward before engaging in criminal conduct.

The message to the public is unmistakable: No fraudster will be treated differently just because of his or her education or corporate standing. And to potential future defendants the statement is equally clear: As you weigh the pros and cons of criminal conduct, know that the government's resources to come after you are immense and the punishment if you're caught will be crushing. And thus our society attempts to deter and punish white-collar crime.

But what if everything we think we know about the motivation and decision-making of white-collar criminals is wrong?

The Psychology Of White-Collar Crime

In his ground-breaking book, *Why They Do It: Inside the Mind of the White-Collar Criminal* (New York: Public Affairs, 2016), Prof. Eugene Soltes debunks conventional wisdom and shows through meticulous case studies what those of us who practice in the field of white-collar criminal defense have long understood: The psychology of white-collar crime is different from street crime; and white-collar defendants typically *do not* weigh risk and reward before engaging in criminal conduct.

In today's political climate, to make these points is to invite controversy. Any opinion that suggests that white-collar criminals, especially bankers, should be understood differently from other criminals runs against the deeply held views of large portions of our country and is taken by many to imply that white-collar criminals are therefore less culpable for their crimes. So it's important to note that to discuss the unique psychology of white-collar crime is not to take sides in the debate over whether white-collar crime is more or less harmful to society than street crime or to make a normative statement about the appropriate punishment of financial crime. Rather, it serves to urge that in thinking about white-collar crime—how to deter it and how to prosecute and defend it—we recognize important distinctions and avoid false parallels.

The distinctions are real, at the most basic of human levels. As Professor Soltes notes, a combination of evolution and socialization ingrains deep in the human psyche an aversion to causing suffering in others. The physical intimacy characteristic of street crime typically requires the perpetrator to consciously override that instinct. A mugger sees the fear in his victim's eyes. A burglar forcing his way into a locked home knows, even if not by name, whose property he is looting and whose sense of security he is violating. The psychological cues that tell the actor that he is breaking society's most established norms are unmistakable and must be consciously suppressed.

Physically distant from their victims, the perpetrators of white-collar crime often miss those visceral cues. An investor trading on inside information or a salesman bribing a public official to win a contract may believe that no one is being harmed. For other crimes like price-fixing or accounting fraud, » Page 13

NICOLAS BOURTIN *is a litigation partner and the managing partner of Sullivan & Cromwell's criminal defense and investigations group.*

Preserving Privilege in Government Investigations in Light of **'SEC v. Herrera'**

BY BOYD JOHNSON, BRENDAN McGUIRE AND ALYSSA DaCUNHA

Corporations under investigation frequently decide to share information derived from privileged investigative materials—in particular, interview memoranda—as part of cooperation efforts with the government. But a recent case from the Southern District of Florida makes clear that counsel must tread carefully when assessing whether and how to share that information, as doing so may risk waiving the work product privilege over the underlying materials and potentially their entire subject matter. In a recent order issued in *SEC v. Herrera*, Order on Defendants' Motion to Compel Production from Non-Party Law Firm, *SEC v. Herrera, et al.*, No. 17-20301 (S.D. Fl. Dec. 5, 2017), a federal magistrate judge concluded that a law firm waived privilege over its interview memoranda and interview notes by providing the SEC with "oral downloads" of the interviews, which the court concluded were the "functional equivalent" of disclosing the memoranda and notes.

In terms of practical impact, the decision appears to expand the scope of materials that may be obtained as a result of actual waiver through disclosure, and further blurs the line between subject matter waiver and actual waiver. Both results unfortunately provide potent new tools for litigants seeking to obtain materials previously considered privileged.

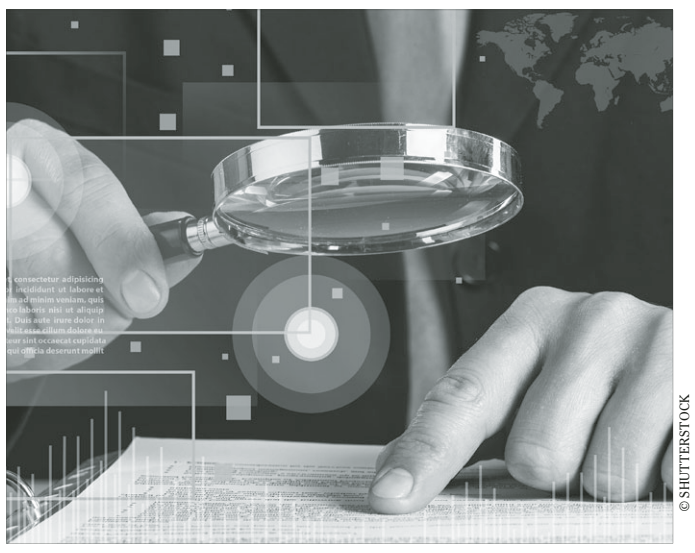
Case Overview

In late 2012, Kentucky-based General Cable Corporation (GCC) identified accounting errors at its Brazilian subsidiary and engaged the law firm of Morgan Lewis & Bockius to conduct an internal investigation. GCC self-disclosed the accounting issues to the SEC, which subsequently launched its own investigation and ultimately entered a Cease and Desist order against GCC in December 2016.

Throughout the course of the investigation, the company cooperated, including by providing oral summaries, or "downloads," of witness interviews to the SEC.

The SEC later brought a civil action against three former GCC employees for their roles in concealing the accounting issues. To "level the playing field," the former employees issued a Rule 45 subpoena to Morgan Lewis seeking production of various materials from the investigation, » Page 10

BOYD JOHNSON *and* BRENDAN McGUIRE *are partners and* ALYSSA DaCUNHA *is counsel at Wilmer Cutler Pickering Hale and Dorr.*



© SHUTTERSTOCK

CFTC 2018 Enforcement: Where the Puck Is Going

BY ZACK BREZ, ALLISON LULLO AND GISELLE SEDANO

Over the last year, the CFTC continued to align itself with other, more frequently-lauded enforcement agencies like the U.S. Department of Justice (DOJ) and U.S. Securities and Exchange Commission (SEC). Among other undertakings, the CFTC implemented new rules aimed at protecting and incentivizing whistleblowers (see CFTC Strengthens Anti-Retaliation Protections for Whistleblowers and Enhances the Award Claims Review Process, May 22, 2017); restructured the market surveillance unit so that it reports directly to the Director of Enforcement (see Testimony of J. Christopher Giancarlo, Chairman U.S. Commodity Futures Trading Commission before the House Committee on Agriculture, Oct. 11, 2017); and issued new cooperation and self-reporting advisories in line with other agencies such as the DOJ, which recently formalized its cooperation-centered Foreign Corrupt Practices Act enforcement policy (id.).

But the CFTC also closed out its fiscal year having brought only 49 enforcement actions, nearly 30 percent fewer actions than in FY2016, and obtaining orders totaling approximately $412 million in restitution, disgorgement and penalties, amounting to only one-third of the $1.29 billion garnered in FY2016. See Commodity Futures Trading Commission Fiscal Year 2017 Agency Financial Report. The low numbers, however, are not all that surprising given the current administration's focus on regulatory minimalism and CFTC Chairman Christopher Giancarlo's parallel mission to "right-size" the agency's regulatory footprint. See Remarks of Acting Chairman J. Christopher Giancarlo at 42nd Annual International Futures Industry Conference in Boca Raton, FL, "CFTC: A New Direction Forward," March 15, 2017. Early last year, Giancarlo launched Project KISS, for "Keep It Simple, Stupid," which directs CFTC staff to review agency rules and apply them in simpler ways. See CFTC Requests Public Input on Simplifying Rule, May 3, 2017. The project's announcement came on the heels of an executive order issued by President Trump calling on federal agencies to find ways to ease regulatory burdens on the U.S. economy.

For the CFTC, perhaps the method for easing those burdens lies in its other FY2017 initiative: getting in step with the ever-evolving, technology-centric markets it polices. As recently as November, Giancarlo reaffirmed to a FinTech-focused audience that the CFTC's mission is to formulate policy around market innovations and use technology to become a more effective and efficient regulator. See Remarks of Chairman J. Christopher Giancarlo at Singapore FinTech Festival, Nov. 15, 2017. To that end, the CFTC launched LabCFTC, a New York-based FinTech initiative tasked with making it easier to align CFTC rules with today's technologies; or, as Giancarlo put it, combatting the CFTC's status as "an analog regulator of rapidly digitizing global markets." Id.

Earning its reputation as the enforcement buzz word of 2017, spoofing is a common form of market manipulation and an attractive target for financial enforcement agencies.

In discussing the LabCFTC initiative, Giancarlo explained that its goal echoed that of hockey legend Wayne Gretzky, who once stated that instead of skating to where the puck was, he skated to where the puck was going. In that same vein, this article discusses the technology-driven trends we anticipate seeing in the CFTC's 2018 enforcement efforts in the three traditional brackets of CFTC actions: (1) trading, (2) Futures Commission Merchants (FCMs), and (3) off-exchange activity. In each of these spaces, we expect to see technological advancements as both the genesis of misconduct as well as the vehicle through which the CFTC will address it.

Trading: Spoofing

Earning its reputation as the enforcement buzz word of 2017, spoofing is a common form of market manipulation and an attractive target for » Page 12

ZACK BREZ *and* ALLISON LULLO *are partners, and* GISELLE SEDANO *is an associate, at Kirkland & Ellis.*

Inside

WHITE-COLLAR CRIME: Angela Turturro, Sections Editor | Agnieszka Czuj, Design

Outside Counsel May Face Criminal Liability In Complex Business Cases

BY TODD BLANCHE AND KYLE DEYOUNG

© SHUTTERSTOCK

When a complex transaction directed by a CEO or CFO is later deemed criminal and the executive is charged, what exposure could outside counsel face having advised and presumably approved the transaction? Similarly, when working with high-ranking executives at a company, when does outside counsel have an obligation to report and update a company's board of directors regarding their work for the CEO on behalf of the company?

Serving as outside counsel can be a minefield, and when the prospect of criminal liability emerges, outside counsel beware. As the recent conviction of Martin Shkreli's outside counsel, Evan Greebel, shows, sometimes counseling clients on transactions that are later deemed to be illegal can cause the government to view outside counsel as a co-conspirator, as opposed to trusted advisor.

The government alleged that Greebel "greased the wheels" for Shkreli and did Shkreli's "dirty work" in order to increase his own compensation at his law firm. Of course, most outside counsel would describe at least some of what they do as "greasing the wheels" for clients, and doing some of the "dirty work" that goes along with running a successful business. But, the difference in the Greebel case is that the government offered evidence, which the jury ultimately accepted, that Greebel helped Shkreli not as outside counsel, but as co-conspirator. According to the government, Greebel helped Shkreli, the CEO of Retrophin, keep certain stakeholders and board members of the company in the dark about material challenges and assisted Shkreli in compensating investors who lost money in a prior hedge fund by creating "sham" consulting agreements with Retrophin. Thus, Greebel went from outside counsel to partner in crime, even though much of his conduct was consistent with work outside counsel do every day.

Walking the Tightrope As Outside Counsel

We, as lawyers, are bound by: (1) ethical duties to not knowingly help clients violate the law; (2) a duty to be zealous advocates for our clients; and (3) the legal duty not to break the law. We are also taught to balance zealous advocacy for our clients with legal responsibilities. We are, after all, considered by many as the gatekeepers to maintaining a clean business environment. These general maxims, however, provide little specific guidance when trying to advise clients that are structuring transactions in a manner that takes advantage of loopholes or permissive laws. Trying to walk the tightrope between a commitment to aggressive clients while not subjecting oneself to potential personal liability for violating the law, presents unique legal risks for outside corporate attorneys.

Most concerning is that when the United States Attorney's Office comes calling, there is little room for error. Advising clients that a particular course of action does, or does not, violate the law is something that lawyers do every day—indeed it is our job! But what stops this advice and counsel from being labeled part of a conspiracy, especially if outside counsel believes that a particular course of action *does not* violate the law and a grand jury later disagrees?

The answer is, alas: it depends. Certainly being careful and thoughtful in the advice given and the work performed is a must. Understanding the reason for the course of action, and knowing the background on why such course is necessary, is also of tantamount importance. In addition, transparency throughout the process, as discussed below, is key to rebutting a later charge of illegally conspiring with your client.

DOJ Is Targeting Outside Counsel in Criminal Prosecutions

While the government targeting outside counsel is not new, outside counsel traditionally received the benefit of the doubt when investigations focused on their clients. However, that tradition is changing as the DOJ broadens the range of actors accountable for a corporation's illegal acts. As outside counsel's responsibilities have broadened, the risk of criminal liability has concomitantly increased. Safe harbors that once existed, such as claiming that counsel only advised a client on business matters, have evaporated, with clients involving outside counsel more and more in business decisions that structure corporate transactions. As the recent prosecutions of attorneys in the EDNY and SDNY demonstrate, the government is comfortable characterizing, and prosecuting, outside counsel as co-conspirators.

Today, government regulators—particularly the DOJ—are not sympathetic to outside counsel when their clients are criminally charged if the indicted client involved outside counsel in all phases of business decisions. Outside counsel serves many hats: a pioneer capable of weaving around compound regulatory issues, a tactician that outsmarts the adversary in litigation, and a visionary capable of engineering a client's path for success. In turn, outside counsel must manage a client's business not in isolation, but as an influencer who is held accountable for the sanctity of our business communities. With the added tension of playing company protector and public servant, outside counsel must carefully advise clients on the outer boundaries of business matters and remain mindful that they are working under the government's watchful eye.

The obvious case of outside counsel turned criminal defendant is the attorney who, for example, knowingly participates in a client's criminal scheme to defraud a company and its investors. But the more complicated story is when outside counsel unwittingly assists in a criminal scheme because the client is not truthful or does not provide all relevant information, thus leaving outside counsel as the client's pawn in his unlawful conduct. Government investigators believe that outside counsel should understand historical reasons for the transaction, act as facilitator and investigator, and probe alternate sources for information that may render the transaction improper. It can be a tough sell to a federal prosecutor who has exposed the CEO's massive fraud when outside counsel sheepishly says, "I didn't know."

> DOJ's investigations and prosecutions of outside counsel who allegedly conspired in a client's criminal activity highlights **a trend in criminal enforcement of business decisions.**

Pitfalls to Avoid as Corporate Outside Counsel

DOJ's emphasis on investigating and prosecuting outside counsel for their involvement in business decisions that ultimately turn criminal is real. Outside counsel should understand the following pitfalls to help avoid criminal liability:

Communication to Stakeholders: Transparency Matters. Disclosure and transparency can help protect the client and outside counsel from liability, but it can be difficult to assess *when* and *to whom* to disclose. When representing public and private companies, outside counsel generally serves at the behest of investors, employees, or the board. Although outside counsel may work primarily for the CEO, the general counsel, or other high ranking executives, their duty is to the company. In the day-to-day grind of working closely with a small group of contacts (likely the people who hired outside counsel), it is easy to forget that the client is the company.

Outside counsel, then, must remind themselves that transparency through disclosure and updates to responsible parties is paramount to avoiding second guessing by others at the company when the DOJ starts asking questions. If the government later claims that the CEO acted illegally but outside counsel regularly updated the board, CFO, or the general counsel about the work he or she is doing, the likelihood of outside counsel being accused of conspiring with the bad actor decreases. If Greebel regularly updated the board of directors at Shkreli's new company about the work he was doing for Shkreli, their CEO, would the government have charged Greebel? Suffice to say the government's proof would have been much different had Greebel regularly updated the board about some of the conduct that was later part of the conspiracy between Greebel and Shkreli.

Furthermore, common sense should always help guide outside counsel's recommendation and best practices for transparency with stakeholders and disclosure obligations to regulators. Disclosure processes require that outside counsel understand their client's business, account for applicable laws and regulations, and consider company information specific to the matter at hand. Because the decision to disclose and what to disclose is not one-size-fits-all, outside counsel must draw from company-specific knowledge and industry norms to help guide clients through sometimes fickle disclosure rules. Altogether, this set of considerations helps shape outside counsel's advice to ensure that a company plays by the rules—and that counsel does not draw the ire of criminal authorities if things go wrong.

Avoid Cognitive Dissonance. Good lawyers care deeply about their clients and zealously advocate on their behalf. We are in a client-service driven industry and want our clients to be satisfied with our work. But lawyers must maintain perspective, always conscious that a client's decision may have severe ramifications for the client, stakeholders, and in extreme cases, for outside counsel.

Accordingly, outside counsel should avoid the culture of cognitive dissonance—a lawyer's natural inclination to alter one's personal beliefs to align with the arguments for which he advocates on behalf of a client. To counter a lawyer's dissonance and to protect one's self from criminal liability, outside counsel must ask hard questions of their clients. Hard questions present genuine risks for attorneys because clients might confuse those questions for distrust and destroy the fabric of a relationship that requires trust. Still, outside counsel should be comfortable asking their clients "why?" and "are you telling me everything here?" at crucial steps of their representation. Also, the classic two-lawyer rule applies well in complicated transactions: ask a trusted colleague if there is something you are missing or if there is a question you should ask your client. A fresh perspective can be useful to counter cognitive dissonance and can further distance a lawyer from hindsight allegations of conspiring.

Conclusion

DOJ's investigations and prosecutions of outside counsel who allegedly conspired in a client's criminal activity highlights a trend in criminal enforcement of business decisions. This hardline stance reinforces outside counsels' professional and legal responsibilities and serves as a reminder that criminal liability might hinge on a client's conduct. But we as lawyers should not tiptoe around clients' issues for fear that our advice will produce the next newspaper headline about an attorney turned conspirator. Rather, outside counsel should become even more assertive in the attorney-client relationship and take more seriously the role as trusted advisor, advocate, and investigator.

TODD BLANCHE *and* KYLE DEYOUNG *are partners at Cadwalader, Wickersham & Taft.* STEPHEN WEISS, *an associate, assisted in the drafting of this article.*

Privilege

« *Continued from page 9*

including interview memoranda. The employees later filed a motion to compel production of the memoranda, arguing that Morgan Lewis waived privilege by providing oral summaries to the SEC. Morgan Lewis argued in response that verbally conveying information from witness interviews to the SEC did not waive work product protection for the underlying memoranda.

The magistrate judge ruled for the employees, concluding that there was "little or no substantive distinction for waiver purposes" between providing the memoranda and orally summarizing the substance of the memoranda. The court observed that waiver issues require an evaluation of the circumstances surrounding the disclosure, and noted that Morgan Lewis went beyond providing "vague references" or "detail-free conclusions or general impressions," and instead provided downloads of the substance of the interviews. Concluding that Morgan Lewis waived work product protection by providing oral downloads of the memoranda to the SEC, the court ordered the firm to disclose not only the memoranda associated with the interviews but also the underlying attorney notes upon which the memoranda were based.

The court rejected the other arguments raised by the former employees. Specifically, the court concluded that neither a PowerPoint presentation made to the SEC nor disclosure of interview memoranda to GCC's auditors resulted in a work product waiver. Notably, no waiver was found with respect to the PowerPoint presentation based on the court's finding that the presentation contained only facts, including the names of the interviewees, and not attorney mental processes.

Implications and Takeaways

The *Herrera* decision is the latest in a line of cases where courts have held that the verbal disclosure of the substance of interview memoranda waives work product protection for the memoranda themselves. For counsel conducting internal investigations, this finding further complicates efforts to cooperate with government inquiries while simultaneously preserving a critical privilege.

Perhaps more importantly, the decision appears to break new ground by concluding that merely providing a summary of the content of interview memoranda resulted in work product waiver of not just the memoranda, but also the underlying attorney notes. Because subject matter waiver is generally disfavored, litigants and government agencies increasingly have been attempting to expand the scope of materials that can be obtained as a result of actual waiver (i.e., waiver through physical disclosure or the oral equivalent). A litigant who can establish actual waiver will almost always be entitled to obtain the materials, so the recent push towards a broad interpretation of actual waiver is a troubling development for counsel seeking to protect attorney work product materials in internal investigations. By adopting an expansive view of actual waiver, the *Herrera* court provides litigants and government agencies with a new and potentially powerful strategy for seeking broad discovery of work product materials.

The result could be a Hobson's choice for a company that seeks to cooperate with a government inquiry: cooperate fully with the government and risk a finding of work product waiver in related litigation or protect your work product privilege and risk the government concluding that your cooperation is insufficient. Moreover, Deputy Attorney General Rod Rosenstein stated in a recent speech that, in the FCPA context, there is now a presumption of a DOJ declination in cases where, among other things, the company voluntarily self-discloses and fully cooperates. To the extent this new policy creates an additional incentive for companies to disclose privileged materials to obtain cooperation credit, *Herrera* makes clear that taking that step may have serious consequences for related litigation.

> The 'Herrera' decision is **the latest in a line of cases** where courts have held that the verbal disclosure of the substance of interview memoranda waives work product protection for the memoranda themselves.

Recommendations

Given the panoply of risks facing companies cooperating with government inquiries, counsel would be wise to consider proactive measures to preserve work product privilege and maximize protection of sensitive investigative memoranda and materials. The *Herrera* order (and cited cases) suggest that there may be ways to successfully navigate these challenging circumstances.

First, the *Herrera* court suggested that merely providing the government with oral high-level conclusions or impressions from the interviews would not result in work product waiver. Similarly, an unpublished S.D.N.Y. decision cited in the order noted that providing general impressions of interviews without organizing them into witness-specific presentations likely would not result in waiver. *SEC v. Vitesse*, 2011 WL 2899082 at *3 (S.D.N.Y. July 14, 2011). Thus, while neither decision established the level of specificity required to trigger a waiver finding, it appears that counsel could preserve privilege by providing high-level conclusions based on the interviews rather than detailed summaries of individual interviews.

Second, it is important to keep in mind that the historic facts at issue in the investigation are not privileged. As a result, presentations to the government that focus on those facts, rather than the substance of witness interviews, should not result in a waiver. The *Herrera* court recognized this, concluding that the PowerPoint presentation for the SEC did not contain the substance of any witness statements and therefore did not implicate the work product privilege.

Of course, government agencies historically have taken a mixed view of whether mere factual presentations represent sufficient cooperation, especially under the previously-issued Yates Memo. But there is a strong argument that providing relevant facts through presentations—without resorting to providing information that may result in work product waiver—accords with DOJ and SEC guidance and should be considered full cooperation. The U.S. Attorney's Manual (USAM) addresses this point, noting that while cooperation credit requires "timely disclos[ure] [of] the relevant facts about the putative misconduct," it does not require disclosure of privileged materials. USAM 9-28.720. Indeed, the USAM specifically states that to receive cooperation credit "the corporation need not produce, and prosecutors may not request, protected notes or memoranda." USAM 9-28.720 (FN 2). This demonstrates that cooperation through sharing facts—rather than interview summaries—should be more than sufficient for DOJ's purposes.

Finally, counsel should attempt to reach an agreement with the government prior to disclosing information from privileged materials. Confidentiality agreements will not necessarily be sufficient to protect work product materials that are turned over to the government, particularly where the government agency has the ability to disclose the materials to others. But counsel may be able to obtain greater protection for oral presentations by reaching an agreement in advance with the government that the proffer of information will not result in a waiver of underlying work product materials. The ultimate impact of such an agreement in persuading a judge presiding over parallel civil litigation of course cannot be guaranteed.

Conclusion

Moving forward, companies and their counsel will need to closely monitor the emerging trend towards a broad interpretation of actual waiver in this area, and be alert to any situations in which sharing information with the government may give rise to a claim of waiver. While not a panacea, carefully tailored factual presentations and explicit confidentiality agreements may enable counsel to maximize protection for work product materials. Companies facing government scrutiny ultimately may decide that the potential benefits of disclosure outweigh the risks, but counsel should carefully consider all proactive measures before taking that step.

Decisions Highlight **Risk** of **Unintended Implied Waivers of Privilege**


© SHUTTERSTOCK

BY DAVID SIEGAL AND MICHAEL SCANLON

In response to allegations of potentially criminal wrongdoing by a client of your firm, your investigation team has completed its review of the facts. You believe your conclusions position the client to receive cooperation credit from the government, so your plan is to make an "attorney proffer" of your findings to the US Attorney's Office. Such attorney-to-attorney discussions have for decades been a key tool in the kit of the white-collar defense lawyer. These presentations, typically made outside the presence of the client, serve multiple purposes, including demonstrating a desire to be cooperative and an ability to be of assistance, but also to gauge potential scope and depth of the authorities' interest in the subject matter.

If you wish, however, to maintain your client's privilege and work product protections over your investigation results, you should consider the implications of two recent federal court decisions finding attorneys' communications with the government impliedly waived their respective clients' privileges—Chief Judge Beryl A. Howell's opinion in In re Grand Jury Investigation and Magistrate Judge Jonathan Goodman's order in *SEC v. Herrera*. These decisions have sent tremors of varying degrees through this foundational process, and highlight the risk that certain communications with government officials may result in unintended (and potentially sweeping) implied waivers of privilege. *In re Grand Jury Proceedings*, Misc. Action no. 17-2336 (BAH), 2017 WL 4898143 (Oct. 2, 2017) (Howell, C.J.); *SEC v. Herrera*, Case No. 17-20301-Civ. Lenard/Goodman, 2017 WL 6041750 (Dec. 5, 2017) (Goodman, M.J.). Judge Goodman in particular was cognizant of the broader implications of his finding of waiver, noting at the outset:

> This Order concerns the legal consequences, if any, which arise when a major law firm conducting an internal corporate investigation into its client's financial and business activities produces what the parties here call "oral downloads" of witness interview notes and memoranda to the regulatory agency investigating its client.

Though distinct in their impact, each of these rulings presents important lessons and considerations for corporate white-collar practitioners in the modern era.

Background

The present-day law of implied waiver grew out of a series of governmental voluntary disclosure programs that fostered what critics have called a "culture of waiver." See Robert J. Anello & Richard F. Albert, "Government Makes Manafort's Lawyer a Key Witness Aginst Him—Ho-hum?," 258 N.Y.L.J. No. 107 (Dec. 5, 2017). Even under the Department of Justice's current guidelines for prosecuting corporate crimes, while prosecutors may not request "non-factual or 'core' attorney-client communications or work product," companies must nevertheless disclose "the facts known … about the putative criminal misconduct under review" to obtain cooperation credit. Office of the U.S. Att'y, U.S. Att'y Manual §9-28.710 (New Aug. 2008). Satisfying the government's cooperation requirements may involve, as a practical matter, describing in substantial detail who said what and to whom, and which witnesses observed which facts. In attempting to meet these demands, defense lawyers can easily find themselves skirting the line of revealing privileged aspects of their work in an effort to obtain the benefits of cooperation. *In re Grand Jury Proceedings*, 219 F.3d 175, 190 (2d Cir. 2000).

The risks associated with privilege waivers are high. Most jurisdictions have rejected the "limited waiver" doctrine—i.e., the notion that a disclosure of privileged information made as part of an effort to cooperate with the government would not constitute waiver as to third parties. Thus, a voluntary waiver to the government is a waiver to all. *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 235 (2d Cir. 1993) (refusing to adopt the selective waiver theory, but declining to a per se rule against it); see also *In re Qwest Commc'ns Int'l*, 450 F.3d 1179, 1186-1201 (10th Cir. 2006) (rejecting theory and collecting cases); *Diversified Industries v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (en banc) (accepting theory). In addition, under Rule 502(a) of the Federal Rules of Evidence, an intentional waiver extends not just to materials actually disclosed to an "adversary"—e.g., the government—but also to *undisclosed* materials on the same subject matter if "they ought in fairness to be considered together." Fed. R. Evid. 502(a). (A finding of fairness typically requires a showing that the disclosing party either made offensive use of protected materials, such as invoking an advice-of-counsel defense, or caused "a selective and misleading presentation of evidence to the disadvantage of the adversary." Fed. R. Evid. 502, advisory committee note.) In making an attorney proffer with sufficient detail to convince prosecuting attorneys of the client's willingness to be cooperative, practitioners run the risk of waiving privilege by including too much detail from their interview notes or memoranda.

'SEC v. Herrera'

The decision in *SEC v. Herrera* arose out of an enforcement action against two former officers of General Cable, a global manufacturer of wire and cable products, who allegedly concealed the manipulation of accounting systems at the company's Brazilian operations. The company discovered the accounting errors before the SEC caught wind of them. It retained outside counsel, Morgan Lewis & Bockius, to conduct an internal investigation, which included interviewing dozens of the company's employees and officers. Later, SEC staff began their own inquiry, and in response to SEC requests, Morgan Lewis produced historical documents to and from the defendants and other persons interviewed, met with SEC staff and presented a PowerPoint setting forth its investigative steps and factual findings, and provided "oral downloads" of twelve witness interviews. The former officer defendants subpoenaed production of, among other things, Morgan Lewis's written notes and memoranda of the witness interviews that the firm had described (though never provided) to the SEC, as well as those additional interviews referenced in the PowerPoint.

> These decisions are recent examples of courts' willingness to order detailed production of otherwise privileged communications when attorneys have described their client communications to government agents.

Morgan Lewis resisted production of the notes and memoranda, arguing work product protection still applied because even those orally described in detail were never actually produced to the SEC. Magistrate Judge Goodman disagreed, concluding that the firm's oral disclosures were the "functional equivalent" of production of the documents themselves. Id. at *6 (emphasis omitted). (Magistrate Judge Goodman also noted the outcome likely would have been different had Morgan Lewis provided "only vague references" to the witness notes and memoranda or "detail-free conclusions or general impressions" of its investigation. Id. at *5, citing *B.M.I. Interior Yacht Refinishing v. M/Y Claire*, No. 13-62676-CIV, 2015 WL 4316929 (S.D. Fla. July 15, 2015)). The court stopped short, however, of ruling that Morgan Lewis's presentations created a wider, subject matter waiver. The PowerPoint (which had already been made available to the defendants) was expressly prepared for the SEC and, therefore, was never itself protected under the work product doctrine, nor did it provide the substance of the additional interviews. Thus, according to the court, fairness considerations required production of the written interview notes and memoranda of the 12 recounted interviews, but not the other interviews incidentally referenced the PowerPoint.

'In re Grand Jury Investigation'

The *In re Grand Jury Investigation* decision arose not from an attorney's proffer, but from a lawyer's letters to the government that became a subject of the Special Counsel's Office (SCO) investigation into potential collusion between U.S. citizens and foreign government actors to influence the 2016 presidential election. The SCO uncovered evidence that Paul Manafort, his lobbying company, and its employee submitted false statements in two letters submitted in November 2016 and February 2017, respectively, to the Foreign Agent Registration Act Registration (FARA) Unit in violation of 18 U.S.C. §1001(a) and 22 U.S.C. §618(a). In the November 2016 submission, the attorney wrote » Page 13

DAVID SIEGAL *is a partner and* MICHAEL SCANLON *is an associate at Haynes and Boone.*

ICO Enforcement Actions
In 2017 and Trends for 2018

BY CHRISTIAN EVERDELL

This past year has seen an explosion of interest and investment in initial coin offerings (ICOs), a new method of raising capital in which startups issue digital tokens to investors, usually in exchange for virtual currency. According to Coinschedule, a website that tracks ICO statistics, there were 235 ICOs that raised over $3.7 billion in 2017. That represents a dramatic increase from 2016, in which there were only 46 ICOs that raised less than $100 million.

This rapid influx of capital, as well as the persistent hype of enormous profits available for the taking, has attracted fraudsters and scam artists to the ICO market. The promise of outsized returns has lured relatively unsophisticated investors, who are hoping to ride the surge of rising token values to turn a quick profit. These investors are easy prey for scammers, who can quickly draft a fraudulent "white paper" outlining a purported startup project, sprinkle it with impressive sounding tech jargon and buzz words like "blockchain," and capitalize on the investors' exuberant hopes for a large and speedy return on their investment to defraud them. At a conference in September 2017, SEC Co-Director of Enforcement Steven Peikin likened these fraudsters to "roaches" that "crawl out of the woodwork and try to scam money off of investors."

As this comment suggests, regulators in the United States recognize the problem and have begun the process of regulating ICO markets and warning investors of the dangers that these investments pose. At the same time, U.S. regulators appear to recognize the potential benefits that ICOs present as a method of raising capital, including the increased access to capital that they provide to digital startup companies who can use them to raise money from a vast pool of retail investors at an early stage of development. The regulators' dilemma, therefore, is to enact a regulatory framework for ICOs that is robust enough to protect investors against fraud and ensure transparency in the marketplace, but is not so onerous that it suffocates innovation and causes ICO issuers to abandon the U.S. market entirely.

The SEC was first to step into the regulatory breach by issuing the "DAO Report" in July 2017, which clearly announced to the market that tokens would be regulated as securities under existing federal securities laws if they qualified as an "investment contract" under the so-called "*Howey* test" set forth in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). At the same time, it signaled that the SEC would proceed carefully and take a case-by-case approach to its enforcement efforts. The question after the release of the DAO Report was: Now that the SEC has stepped in, how exactly will it police the ICO marketplace?

Thanks to a series of enforcement actions that the SEC brought in the last two quarters of 2017, we now have some preliminary answers. The SEC appears to be pursuing a deliberately measured enforcement strategy by initially targeting ICOs that involved obviously fraudulent conduct or where the token was clearly marketed as a security. For the moment, the SEC is steering clear of more complicated ICOs where the *Howey* analysis is less clear. In other words, the SEC is going after the low-hanging fruit first—a trend that will likely continue in 2018.

It is more likely that the thornier securities law issues will be tackled initially by federal courts in connection with private securities lawsuits against ICO issuers, the very first of which were filed in the last few months of 2017. It is fair to assume that these lawsuits will only increase in 2018, and will further clarify the legal landscape in this area.

RECoin, PlexCoin, And Munchee: The SEC's Opening Salvo

Having set the expectations of the market with the DAO Report, the SEC's enforcement strategy began in earnest on Sept. 25, 2017, when it announced that it had created a new Cyber Unit that would focus on cyber-related misconduct, including ICO violations. The SEC followed its announcement a few days later by bringing its first enforcement action against two ICO issuers called RECoin Group Foundation (RECoin) and DRC World (DRC), as well as the man who allegedly controlled them both, Maksim Zaslavskiy. In December 2017, the SEC filed two additional enforcement actions against PlexCorps and its founder Dominic Lacroix, and against Munchee.

The RECoin case and the PlexCorps case were similar in that they both involved allegations of outright fraud. According to the SEC's complaint, RECoin and DRC claimed that they would use the proceeds raised by the ICO to purchase, respectively, real estate and diamonds, which would back the tokens causing them to "grow" or "increase" in value over time. In fact, according to the SEC, Zaslavskiy never bought any real estate or diamonds, nor did he even develop a token that RECoin or DRC could provide to their investors. Similarly, the SEC alleged that PlexCorps made numerous misrepresentations in marketing the PlexCoin token. For example, the PlexCoin white paper promised investors returns of 1,354 percent in "29 days or less." In fact, according to the SEC, PlexCoin was a fabrication and Lacroix and his girlfriend used the proceeds from the PlexCoin ICO for "extravagant personal expenditures."

© SHUTTERSTOCK

> Whereas 2017 set some basic guardrails around the ICO market, **2018 will likely see an increase** in regulatory activity by multiple agencies, and a deeper engagement with the difficult legal questions posed by ICOs.

The Munchee case, which involved a company that created an iPhone app for people to review restaurant meals, was slightly different because it did not involve allegations of fraud. Instead, it was designed to put a shot across the bow of ICO issuers who market so-called "utility" tokens.

Since the release of the DAO Report, numerous ICO issuers have attempted to circumvent the application of the securities laws by claiming that their tokens are not securities because they are not investments that return a profit. Instead, they claim that the value of their tokens is derived solely from their "utility" on the platform for which they were designed. Munchee, for example, stated that restaurants that purchased its MUN token could later use the tokens to buy advertising on the Munchee "ecosystem." The MUN white paper even claimed that Munchee had done a "*Howey* analysis" and concluded that "the sale of MUN utility tokens does not pose a significant risk of implicating the federal securities laws." At the same time, Munchee touted the profit potential of MUN tokens, claiming that MUN tokens would increase in value and emphasizing that users would be able to trade them on a secondary market.

The SEC saw through this obvious fig leaf and obtained a cease-and-desist order against Munchee, which stated unequivocally that MUN tokens were securities despite Munchee's efforts to label them as "utility" tokens. SEC Chairman Jay Clayton delivered this same message to the broader ICO market in a statement issued that same day: "[m]erely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security."

The Outlook for 2018

These three enforcement actions represent the SEC's opening salvo in the ICO arena, and are entirely consistent with the measured, case-by-case approach signaled by the DAO Report. Each of these cases involved relatively straightforward applications of the *Howey* test, and two involved allegations of blatant fraud. They indicate that the SEC is serious about policing ICOs, but is deliberately trying not to overreach by diving into the middle of a complicated marketplace. For the time being, the SEC seems focused on quickly imposing a basic level of security and transparency in the ICO market by containing the worst actors and setting some clear boundaries around what constitutes a security.

What is the enforcement outlook for 2018? Already there are some trends to watch. First, the SEC is no longer the only agency regulating ICOs. In October 2017, the CFTC announced that tokens issued through ICOs may be considered commodities. State securities regulators have also thrown their hat into the ring. In the first week of January 2018, the Texas State Securities Board blocked a token sale by BitConnect on the grounds that it was marketing an unregistered security under Texas state law.

Second, private litigants have begun filing the first securities class actions lawsuits against ICO issuers. Already Tezos and GigaWatt, each of which had lucrative ICOs in 2017, have been sued by token holders for alleged securities law violations. These private suits are intriguing because the tokens that were marketed in these ICOs do not bear the same obvious hallmarks of securities as RECoin, PlexCoin and the MUN token, making the *Howey* analysis much more complex. It is therefore likely that the federal courts, and not the SEC, will take the lead in resolving the more difficult securities law questions surrounding ICOs in the coming year.

Whereas 2017 set some basic guardrails around the ICO market, 2018 will likely see an increase in regulatory activity by multiple agencies, and a deeper engagement with the difficult legal questions posed by ICOs.

CHRISTIAN EVERDELL *is a member of Cohen & Gresser's white-collar defense group.*

CFTC

« Continued from page 9

financial enforcement agencies. See Q&A—Interpretive Guidance and Policy Statement on Disruptive Practices. Spoofing is most often executed via complex computer algorithms that rapidly display and then cancel bids or orders so that the spoofer may advantageously buy low and sell high, or vice versa. Id. Although there have been cases brought against "manual" spoofers, the majority of CFTC and Exchange enforcement actions against spoofers involve automated spoofing. See IMPACT ANALYSIS: Nasdaq publishes white paper, suggestions for detecting spoofing, July 5, 2017, Reuters. Cf. CFTC Orders New York Trader Simon Posen to Pay a $635,000 Civil Monetary Penalty and Permanently Bans Him from Trading in CFTC-Regulated Markets for Spoofing in the Gold, Silver, Copper, and Crude Oil Futures Markets, July 26, 2017 (trader "manually placed orders to buy and sell gold, silver, copper, and crude oil futures contracts with the intent to cancel these orders before execution (spoof orders)"). During FY2017, the CFTC brought nine actions involving spoofing, imposing $27.35 million in aggregate penalties and permanent trading and registration bans. See Commodity Futures Trading Commission Fiscal Year 2017 Agency Financial Report. Only one of these actions stemmed from self-reporting, whereas the remainder resulted from market regulation efforts. See CFTC Finds that The Bank of Tokyo-Mitsubishi UFJ, Ltd. Engaged in Spoofing of Treasury Futures and Eurodollar Futures, Aug. 7, 2017; see also id. Detecting spoofing requires reviewing the market context, an individual's trading activity patterns, and other pertinent facts and circumstances. But advancements in technology and automation have armed would-be spoofers with stealthier methods of manipulation, making the increasingly electronic marketplace more difficult to surveil. Automated trading now constitutes up to 70 percent of regulated futures markets and foreign exchange spot markets, and Giancarlo predicts it will continue to dominate with "new and innovative developments far into the future"—which means CFTC's surveillance abilities must follow suit. See Remarks of Chairman J. Christopher Giancarlo at Singapore FinTech Festival; see also Address of CFTC Commissioner J. Christopher Giancarlo to the American Enterprise Institute, "21st Century Markets Need 21st Century Regulation," Sept. 21, 2016.

In implementing a new "big data" platform, the CFTC recognized this growing need to collect and analyze large amounts of data so that it may swiftly take appropriate regulatory action. See Commodity Futures Trading Commission Fiscal Year 2017 Agency Financial Report. The new platform allows CFTC staff to analyze billions of market transactions in a fraction of the time necessary under older systems. For instance, the big data platform now completes a query used to identify spoofing activity in futures market data in approximately seven minutes, instead of the 20 plus hours previously required. Id. The CFTC has also made organizational changes that reflect its desire to employ technology to more quickly and effectively detect and prosecute spoofing. The realignment of the market surveillance unit to sit within the Division of Enforcement was applauded by Giancarlo as a step towards strengthening the agency's prosecution of violations like spoofing. See Remarks of Acting Chairman J. Christopher Giancarlo at 42nd Annual International Futures Industry Conference in Boca Raton, FL, "CFTC: A New Direction Forward," March 15, 2017.

Futures Commission Merchants: Virtual Currencies

Easily the most ubiquitous FinTech innovation of late, the development of virtual currencies—digital representations of value functioning as mediums of exchange, units of accounts, and/or a storage of value—has regulators straining to catch up. See A CFTC Primer on Virtual Currencies, Oct. 17 2017. Virtual currencies are not guaranteed by the central bank or any state body, and therefore pose high risks in terms of price volatility, platform instability, and cyber-threats, including theft, hacking, and loss. See Customer Advisory: Understand the Risks of Virtual Currency Trading, Dec. 15, 2017. Yet believers remain undeterred: Despite plummeting 45 percent in December, the value of popular virtual currency bitcoin more than doubled that same month (see Bitcoin Price: Digital currency had big swings in 2017, Dec. 29, 2017, USA Today), increasing more than 1,900 percent at one point in 2017 and soaring from below $1,000 to almost $20,000 on the CoinDesk Bitcoin Price Index. See From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited, Dec. 29, 2017. Estimates report that the market capitalization of the asset class briefly crossed $600 billion late last year, increasing nearly 3,300 percent in less than one year. See Cryptocurrencies are now worth a grand total of $600 billion—and climbing, Business Insider, Dec. 21, 2017.

But virtual currencies' novelty poses extraordinary challenges for the CFTC, whose jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. See A CFTC Primer on Virtual Currencies, Oct. 17 2017; Customer Advisory: Understand the Risks of Virtual Currency Trading, Dec. 15, 2017. As Giancarlo has observed, "virtual currencies are unlike any commodity that the CFTC has dealt with in the past." See CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange, Dec. 1, 2017. In its first regulatory action targeting virtual currency fraud, in September 2017 the CFTC charged a New York corporation and its CEO and head trader with fraud, misappropriation, and issuing false account statements in connection with a two-year bitcoin Ponzi scheme. Allegedly, the scheme fraudulently raised more than $600,000 for supposed placement in a pooled commodity fund that purportedly operated a high-frequency, algorithmic trading strategy executed by a computer trading program named "Jigsaw." See CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme, Sept. 21, 2017. In connection with the charges, CFTC Director of Enforcement James McDonald credited the exemplary work of LabCFTC as demonstrating the CFTC's "continued commitment to facilitating market-enhancing FinTech innovation" and "acting aggressively and assertively to root out fraud and bad actors in these areas." Id.

Cryptocurrency concerns will undoubtedly remain on the CFTC's agenda in 2018, as the market only continues to grow. In July of last year, the CFTC granted LedgerX registration to clear and custody cryptocurrencies, making it the first U.S. federally-regulated virtual currency derivatives platform and clearinghouse. See Commodity Futures Trading Commission Fiscal Year 2017 Agency Financial Report. In December 2017, both the CME Group Inc. and Cboe Global Markets Inc. launched bitcoin futures contracts, traded under product codes BTC and XBT, respectively, and Nasdaq, Inc. plans to launch its own bitcoin futures in the first half of this year. See Nasdaq Plans to Launch Bitcoin Futures in First Half 2018, Nov. 29, 2017, The Wall Street Journal.

Off-Exchange Activity: Commodity Based Binary Options

The accessibility—and opacity—of the Internet provides an easy opportunity to take advantage of unsophisticated investors eager to enter the market. Binary options, often referred to as "all-or-nothing options," are one such example. Binary options' payout depends entirely on the outcome of a yes/no proposition related to whether the price of a particular asset will rise above or fall below a certain amount at a specified date and time. See CFTC Fraud Advisories, Binary Options. Unlike other options, a binary option does not give the holder the right to purchase or sell the underlying asset. Id. Rather, upon expiration, the holder will receive a pre-determined amount of cash or nothing at all. Id.

The CFTC's jurisdiction encompasses binary options when the transaction involves commodities like foreign currencies, metals, or agricultural products. Any entity soliciting, offering, or accepting offers to enter into commodity-based binary options transactions with U.S. citizens are doing so illegally unless the transactions are conducted on a designated contract market, with limited exceptions. Id. Accordingly, the CFTC maintains a Registration Deficient List (the RED List), which identifies unregistered foreign entities believed to be illegally soliciting and accepting funds from U.S. residents to trade in binary options. See CFTC Publishes List of Foreign Entities that Illegally Solicit U.S. Residents to Trade Foreign Currency and Binary Options, Sept. 9, 2015. In 2017, the CFTC nearly quadrupled the number of entities on the RED List when it added a total of 92 names. See CFTC Adds 21 Names to Its List of Foreign Entities that Illegally Solicit U.S. Residents to Trade Binary Options and Forex, Dec. 15, 2017; see also CFTC Adds 71 Names to Its List of Foreign Entities that Illegally Solicit U.S. Residents to Trade Binary Options and Forex, April 25, 2017.

Much of the binary options market operates through Internet-based trading platforms that do not comply with regulatory requirements. As demonstrated by the CFTC's recent enforcement actions, the pattern is often the same: entities drive potential customers to their websites offering commodity-based binary options, accept customer money, and, rather than trading binary options on customers' behalf, illicitly use the funds for their own expenditure. See, e.g., CFTC Charges California Resident Jason B. Scharf, His Worldwide Web of Companies, and Florida-Based Affiliate Marketers Michael Shah and Zilmil, Inc. with $16 Million Binary Options Fraud Scheme, July 18, 2017; Federal Court Orders Relief Defendants Westward International Ltd. and Coucarin Holdings Ltd. to Disgorge Ill-Gotten Funds Totaling More than $1.77 Million in CFTC Binary Options Fraud Action, April 6, 2017; and Federal Court in Florida Orders Neil Pecker and His Company, Vision Financial Partners, LLC, to Pay More than $6.5 Million in Restitution and a Civil Monetary Penalty in CFTC Binary Options Fraud Action, March 21, 2017. For example, last year, the CFTC charged several individuals and entities for operating a set of binary options websites through which over $16 million was allegedly illicitly solicited and misappropriated from over 8,000 customers. See CFTC Charges California Resident Jason B. Scharf, His Worldwide Web of Companies, and Florida-Based Affiliate Marketers Michael Shah and Zilmil, Inc. with $16 Million Binary Options Fraud Scheme, July 18, 2017. The massive scheme attracted potential customers through fraudulent advertising campaigns, including one with the tagline: "The Most Profitable Click You Will Ever Make." Id. The money customers used to fund their trading accounts was then routed through foreign corporations and overseas accounts in order to pay the business and personal expenses of the charged individuals. Id.

In addition to traditional enforcement, and as promulgated in LabCFTC's goals, the CFTC has collaborated with tech giants to address binary options fraud at its source. For example, CFTC educated the Apple and Google app stores about binary options fraud and identified RED List entities that were selling apps on their platforms. See Commodity Futures Trading Commission Fiscal Year 2017 Agency Financial Report. These efforts led both stores to remove apps that violated their terms and conditions and, in June 2017, Apple voluntarily ceased accepting binary options apps completely. Id.

Conclusion

The CFTC has recognized that it must modernize the ways in which it detects and addresses misconduct in order to keep up with the rapidly advancing, technology-centric markets it is tasked with overseeing. The CFTC's sharp focus on technology is a move designed to understand where the puck is going, and we expect this technology driven approach to continue to shape CFTC enforcement throughout 2018.

Psychology

« Continued from page 9

the victims may be impossible to identify and their individual economic injury so slight as to be imperceptible. As a result, the would-be white-collar criminal, if he stops to consider the question at all, may conclude that with no harm, there can be no foul—this is just the way the business works. The human instinct that warns against causing the suffering of others never kicks in.

This explains why, as Professor Soltes documents, so many white-collar criminals looking back cannot recall having made a conscious decision to engage in crime. Few of them recount having engaged in a careful risk-reward calculus. In many cases, the modest monetary benefits they earn from their crimes could never rationally outweigh the catastrophic consequences to careers and families. Instead of a single dramatic leap, the criminal path of the typical white-collar criminal consists of small, incremental steps—each one perhaps even justifiable on its own—until he finds himself so far over the line that there is no turning back.

Defending Against Intent In White-Collar Prosecutions

What does this mean for a white-collar defense lawyer? With rare exceptions, intent is a bedrock principal of criminal law. No mistake or error in judgment, no matter how inexcusable or how great the consequences, should be punished criminally unless the actor intended to cause the negative outcome—or at least to violate the law. (A host of civil sanctions, including highly punitive monetary penalties and industry debarment, are of course available in cases where wrongdoers acted recklessly or negligently.)

And, as I've written before (Bourtin, Nicolas. "Combatting Hindsight Bias in White-Collar Criminal Investigations," New York Law Journal, April 3, 2017), in financial crime more than in most areas of criminal law, guilt or innocence usually turns not on what the defendant did, but on the defendant's intent in doing it. What was the defendant's state of mind when she approved an accounting treatment, drafted a securities disclosure, or made a representation to a counterparty that now appears incorrect? A defendant's mental state can only be inferred, and the documentary record is often ambiguous.

But if, as Professor Soltes argues, intent is a particularly amorphous concept when it comes to white-collar crime—and if white-collar crime is an area of criminal law where the proof of intent often matters the most—the challenge to our justice system of distinguishing true criminal conduct from innocent errors in judgment becomes extraordinarily difficult. It perhaps explains why prosecutors and the public prefer to adopt the comfortable paradigm of the calculating white-collar criminal.

In the face of that, how does a defense lawyer convincingly make the case that although her client acted consciously and deliberately—and, in hindsight, improperly—he never intended to act criminally? The standard playbook—argue that there is insufficient direct evidence that the client intended to commit an unlawful act—may not be enough. Unless defense counsel can answer the question "How could he not have known?," prosecutors and juries may conclude that the only possible inferences are guilty ones. That's what makes the unique psychology of white-collar crime so important. If defense counsel can explain, in a common-sense, non-academic way, what makes white-collar crime different on the question of intent, she stands a far greater chance of convincing her audience that what may appear fraudulent in hindsight looked very different at the time to a client who never saw and never thought about the people who could be harmed.

In some cases, of course, that hurdle may prove too high. There will be too many emails, false certifications, or other incriminating evidence to avoid the conclusion that the client at some point must have realized that he was committing fraud, even if he didn't set out to. And in many cases, that may indeed be true, and the best legal advice may be to counsel a client to understand that criminal intent can sometimes consist of a series of questionable incremental judgments, even without a moment of conscious decision-making to break the law.

How to distinguish between those two cases is what keeps white-collar defense attorneys awake at night.

Preventing White-Collar Crime

Other important questions follow from Professor Soltes' insights. If tilting the risk-reward calculus in favor of ever greater deterrence will not effectively deter most white-collar crime, and if few white-collar criminals experience that moment of decisional clarity—Do I break the law or don't I?—how can a company create a compliance program that deters unlawful behavior?

There are no easy answers, but at least part of the solution involves training and culture. Compliance training should include efforts to sensitize employees on how to identify potential harm to others, even when that harm is diffuse and the victims faceless and difficult to identify. Employees should internalize the mental exercise of imagining who might be harmed by a particular financial product or business practice.

Companies should also work to develop a culture where respectful disagreement is possible—where "nagging doubts" can be voiced without fear of criticism or reprisal. Employees should be incentivized to raise questions and concerns thoughtfully and respectfully. And leaders adept at encouraging and facilitating the productive, non-confrontational resolution of such concerns should be rewarded and promoted. In this way, no employee will have to operate in an "ethical silo" walled off from the benefit of the collective ethical insights of her colleagues.

Conclusion

Anyone who spends time with white-collar defendants soon realizes that the popular conceptions are almost never accurate. The societal harm white-collar criminals cause can be devastating, but few begin their careers determined to enrich themselves by breaking the law. How and why a white-collar professional came to be a criminal defendant is almost invariably a fascinating and complex question, and the answer is always important—to the defendant himself, to the company where he worked, to the attorney assigned to defend him, and to society at large.

Waivers

« Continued from page 11

that her clients "did not have an agreement to provide services" to a particular foreign entity, and "were not counterparties to any service agreements" between two government relations companies. In the February 2017 letter, written as a "more fulsome explanation" of her clients' work, the attorney wrote that one employee "recall[ed] interacting" with consultants of the foreign entity, but neither employee "recall[ed] meeting with or conducting outreach" on its behalf to U.S. officials or media outlets, and did not "recall" facilitating such communications, but rather, recalled that "such communications would have been facilitated by" the foreign entity.

The grand jury subpoenaed the attorney to testify to the communications underpinning the factual representations in her letters. The attorney refused based on her clients' invocation of the attorney-client and work product privileges. Over multiple filings and three hearings, the SCO clarified that it wanted testimony on the following eight issues:

(1) Who were the sources of the specific factual representations in the letters?

(2) Who were the sources of the email retention policy referenced in and attached to one of those letters?

(3) Did the targets or anyone else at the targeted company approve the letters before the attorney sent them?

(4) What, if anything, did the sources identified in response to the above three questions say to the attorney about statements in the letters?

(5) When and how did the attorney receive communications from the targets, including whether by telephone or email?

(6) Did anyone ask the attorney questions or suggest corrections to the letters?

(7) Did the attorney memorialize her conversations with the targets?

(8) Did the attorney act with care in submitting the letters, and whether it was her practice to review submissions with her clients before sending?

The SCO sought to overcome privilege based on the crime-fraud exception and implied waiver. Chief Judge Howell ruled in favor of the government on both grounds, compelling the attorney's testimony.

The court found the letters had impliedly waived the privilege because they "made specific factual representations" that were "unlikely to have originated from sources other than the Targets, and, in large part, were explicitly attributed to one or both Targets' recollections." Id. at *11. In addition, without citing to Rule 502(a), the court found that the attorney's waiver extended to all her other communications on the same subject matter (id., quoting *In re Sealed Case*, 29 F.3d 715, 719 (D.C. Cir. 1994)), then held that the attorney-client privilege would not prevent her from responding to any of the eight questions. The work product doctrine provided only slightly more protection. After finding that the SCO could take discovery of fact, but not opinion, work product, the court determined that only question number 7 would improperly elicit the attorney's mental impressions or legal theories. She was ordered to answer the other questions.

Takeaways

White-collar attorneys will continue to employ the attorney proffer to advance their clients' interests in responding to investigations, even while on occasion accepting the consequence of some limited waiver of privilege over the facts they strategically divulge. The goal, however, is to minimize the extent to which additional privileged content is swept into that ambit. These decisions are recent examples of courts' willingness to order detailed production of otherwise privileged communications when attorneys have described their client communications to government agents. In practice, attorneys should, to the extent possible, describe factual information without providing witness attribution, and favor reference to preexisting documents rather than after-the-fact interview statements. Quotations from interview notes and memoranda should be kept to an absolute minimum. Practitioners should also seek to cabin the scope of any court-compelled waiver by pointing to the fairness analysis required under Rule 502(a), and Second Circuit precedent requiring district courts to "make particularized findings explaining the connection" between the disclosed information and any additional materials that, in fairness, must be also considered. *In re Grand Jury Proceedings*, 219 F.3d 175, 192 (2d Cir. 2000).