White-Collar Crime

Ways Your Company May Be Drawing **Criminal Health Care Fraud Scrutiny**

© SHUTTERSTOCK

BY MARANDA E. FRITZ, SARAH M. HALL AND JOHN R. MITCHELL

As federal judges in New York and elsewhere continue to hand down decades-plus long prison sentences for health care fraud and the administration increases federal resources devoted to combating health care fraud, health care providers should pay close attention to the "badges of fraud" that may land your company in the crosshairs of a federal criminal investigation.

Below, we look at the "red flags"—the areas of potential fraud of which a health care company should be aware to stay compliant and off the DOJ's radar.

A Hot Enforcement Area

It should come as no surprise to health care professionals that criminal health care fraud enforcement is increasing. The highly successful U.S. Department of Justice Medicare Fraud Strike Force, led by the Fraud Section in Main Justice, has convicted thousands of defendants nationwide, and its last health care fraud "takedown" in July 2017 was the biggest in DOJ history with more than 400 individuals charged. Judges continue to impose lengthy prison sentences, including a 13-year sentence handed down to Dr. Imran Ahmed in February 2018 in the Eastern District of New York.

These stats are only poised to increase as the administration has devoted significant federal dollars to combating health care fraud. The administration's fiscal year 2019 budget request calls for $770 million in anti-fraud funding, a jump from the FY 2018 request of $751 million.

DOJ continues to view criminal health care fraud as a target-rich environment for investigation and prosecution.

The bottom line: DOJ continues to view criminal health care fraud as a target-rich environment for investigation and prosecution.

What Are the Top Red Flags for Health Care Fraud?

As a health care industry GC or executive, you should be on the lookout for any of these red flags in your business practices.

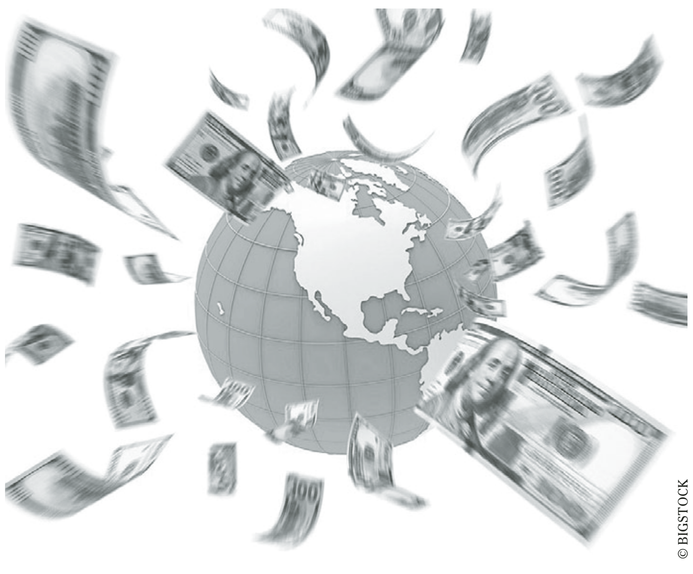
(1) Opioids. Not surprisingly, if you or your company prescribes, sells or distributes opioids, that mere fact alone could warrant scrutiny, given the administration's focus on combating the opioid epidemic. In August 2017, Attorney General Sessions announced the formation of the Opioid Fraud and Abuse Detection Unit, a pilot program that uses data to identify and prosecute individuals engaged in opioid-related health care fraud. The program will fund 12 Assistant U.S. Attorneys, to be located in health care fraud hot spots around the country. These AUSAs will focus on investigating and prosecuting "pill mills," pharmacies that improperly divert and dispense prescription opioids, and other opioid-related issues. Overall, if your practice writes a high number of prescriptions for opioids, that fact alone could spark enforcement interest.

(2) Home Health Care. Home health care fraud has traditionally been a rich area of prosecution for DOJ. Generally speaking, home health care can be prescribed by a doctor when the patient is homebound and needs intermittent skilled care. Traditional flavors of fraud in the home health care sphere have included doctors writing prescriptions for home health care when there is no real medical necessity, unlicensed workers rendering the "care," workers billing for services not rendered ("no-show workers") and kickbacks being paid to recruit patients. If your medical practice includes home health care, be aware that your practices may fall under scrutiny. A recent example of a lengthy prison sentence handed down in this area is the 35-year sentence for Dr. Jacques Roy in Dallas for home health care fraud involving more than 11,000 patients.

(3) More Data, More Problems. For many years, DOJ has used providers' claims data to help identify health care fraud. This data crunching will continue to become more sophisticated over time as more resources are allocated to health care fraud data analytics. Uses of the data range from identifying geographic hotbeds for fraud so enforcement resources can be targeted and deployed to identifying the top doctors who are using billing codes that are suspected to be fraudulent. In this case, being the top biller in the country for a specific code is not a good thing and will almost certainly lead to greater scrutiny. DOJ will zero in on these outliers as a possible badge of fraud, looking for a disconnect between the size of the medical practice and the volume of billing (i.e., a small practice with a large volume of billing), incongruity between the practice's specialty and the types of codes billed (e.g., a general practitioner prescribing a high percentage of opioids), and whether a large portion of the overall claims billed skew toward higher-paying codes even when lower-paying codes are available. The bottom line: Know your data and be able to defend it. If you are a high-volume biller, or if there are anomalies or spikes, you could be targeted.

(4) Robosigning. A common theme among many health care fraud cases is the practice known as "robosigning," which typically involves a doctor blindly writing prescriptions or orders that authorize care without first making an individualized determination of medical necessity. The government will use data analytics and other means to identify possible robosigning, especially when the orders are for expensive drugs or services, or those areas of care that have a track record of inappropriate ordering (such as opioids, home health care, power wheelchairs and sleep studies). Your company should ensure that the authorizing medical professional is actually making a case-by-case analysis of medical necessity before ordering drugs or services. And importantly, the company should be able to re-create and affir- » Page 14

MARANDA E. FRITZ *is a partner in Thompson Hine's New York office,* SARAH M. HALL *is senior counsel in the firm's Washington, D.C. office, and* JOHN R. MITCHELL *is a partner in the firm's Cleveland office. All three authors are former federal prosecutors and members of the firm's white-collar criminal practice, internal investigations and government enforcement practice.*



© BIGSTOCK

OFAC Sanctions: Costly … But Effective?

BY DAVID L. HALL AND DANA STEPNOWSKY

Economic sanctions are touted as a powerful tool in the fight against terrorism, rogue regimes, and transnational criminal organizations. Each round of new sanctions is accompanied by bold assertions of the positive effect the sanctions will have on national security. Critics, on the other hand, contend economic sanctions will cause unintended consequences by harming U.S. business interests or damaging economic relationships with foreign nations. But a more fundamental question goes unanswered: Is the cost to U.S. business *justified* by the benefits of sanctions? In other words, are U.S. economic sanctions programs effective in achieving their stated goals?

OFAC Sanctions: A Little Background

The Office of Foreign Assets Control (OFAC) administers economic sanctions programs focused on rogue regimes, terrorist organizations, and other bad actors that pose a threat to U.S national security and foreign policy objectives. While country-based sanctions programs (such as those imposed against Iran, Cuba, and North Korea) receive attention in the headlines, other programs targeting individuals and entities involved in criminal transactions are imposed with less fanfare. Collectively, these individuals and entities make up the Specially Designated Nationals and Blocked Persons List (the SDN List). The SDN List identifies more than 5,000 individuals and entities blocked under one OFAC sanctions program or another.

SDN designations are consequential. With rare exceptions, all U.S. persons are prohibited from engaging in any transactions with SDN individuals or entities. Additionally, the property and interests in property of any designated person must be blocked if it comes into the United States or into the possession or control of a U.S. person. See, e.g., the Foreign Narcotics Kingpin Designation Act, 31 C.F.R. Part 598.206. The penalties for violation are heavy indeed. The maximum civil penalty for an OFAC violation under the International Emergency Economic Powers Act (IEEPA) is currently $289,238 (or twice the amount of the underlying transaction, whichever is greater). 82 Fed. Reg. 10434 (Feb. 10, 2017). The Kingpin Act has an even higher maximum penalty of $1,437,153 per violation. 31 CFR 598.701. In 2017, OFAC issued penalties or reached settlements with 15 such entities for a total of more than $119 million.

The SDN List is designed to cut off known bad actors and their criminal networks from access to U.S. financial markets, thus crippling their ability to reap the rewards of their criminal actions and to continuing funding their unlawful activities. The effectiveness of these designations, however, depends not on the U.S. government, but on U.S. financial institutions and U.S. businesses in their role as gatekeepers, preventing SDNs from moving funds, making investments, and purchasing goods and services. Paradoxically, it is these gatekeepers—not the blocked parties on the SDN List—that are the targets of OFAC enforcement actions and penalties.

Exacerbating the situation, OFAC sanctions are enforced according to a strict liability standard. Thus, while the highest penalties are reserved for companies that willfully or recklessly commit violations, companies that commit even inadvertent violations are at substantial risk. For example, Richemont North America (d.b.a. Cartier) reached a settlement for $334,800 for engaging in four transactions violating the Kingpin Act by unknowingly selling jewelry to an SDN. See OFAC Enforcement Information for Sept. 26, 2017. In another OFAC enforcement action, Honda Canada Finance, Inc. (HCFI) agreed to pay $87,255 to settle its potential civil liability for approving and financing lease agreements between an unaffiliated Honda dealership in Canada and the Embassy of Cuba after its compliance program failed to flag transactions with Cuba. OFAC Enforcement Information for June 8, 2017.

Do SDN Designations Work?

From the U.S. government perspective, it is not surprising that penalties for violations of OFAC blocking actions are severe; U.S. national security is at stake. On the other hand, it is equally true that there is a great deal at stake for businesses that » Page 14

DAVID L. HALL *is a partner and* DANA STEPNOWSKY *is an associate at Wiggin and Dana.*

The Ninth Circuit's 'Glassdoor' Decision: **Grand Juries** and **Anonymous Speech**

BY MICHAEL GRUDBERG

Every day millions of Americans publish opinions on the Internet; if they do so unnamed or by pseudonym, they can expect to communicate anonymously. Every day prosecutors issue subpoenas to determine whether crimes have been committed; if they do so in reasonable good faith, they can expect those subpoenas will be enforced. These expectations collided last year in *In re Grand Jury Subpoena (Glassdoor)*, No. 17-16221 (9th Cir. Nov. 8, 2017), a closely watched appeal in the Ninth Circuit from an order compelling the operators of an employee-review website to disclose identifying information of users posting anonymous comments about a company subject to grand jury investigation.

The panel upheld the district court, rejecting First Amendment challenges interposed (on users' behalf) in a motion to quash. The opinion has drawn thoughtful commentary, regarding the tension between the public's interest in the prompt investigation of crime and the right to anonymous expression. Although litigation over anonymous online speakers is unlikely to be settled by this controversy alone, there are reasons to expect (or hope) that prosecutors will pursue other avenues to locate persons with knowledge of corporate fraud, and that the compelled outing of commentators might remain an unusual last resort.

Background

The controversy arose from an investigation by the Arizona U.S. Attorney into the operations of a government contractor administering two VA healthcare programs. The government served a subpoena on Glassdoor, operating the "Glassdoor.com" website, where employers promote job openings and employees rate the companies on working conditions and benefits. Reviewers post to the site anonymously. The subpoena sought every "company review" regarding the subject contractor, together with names, addresses and identifying data of the reviewers. There were 125 postings, but the government agreed after discussions to limit its request to eight reviews, critical of the contractor, that were attached to the subpoena.

Despite the government's trimming, Glassdoor moved to quash based on its users' rights to anonymous speech. The district court denied the motion, relying on *Branzburg v. Hayes*, 408 U.S. 665 (1972), in which the U.S. Supreme Court held that reporters must cooperate with a grand jury, in spite of anonymity promises to sources, where the government probe is not under- » Page 15

MICHAEL GRUDBERG *is a partner at Tarter Krinsky & Drogin.*

Inside

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

'People v. Weinstein': New York Attorney General's Sharp Warning About Systemic Workplace Sexual Harassment

BY ROSS M. KRAMER
AND SUZANNE JAFFE BLOOM

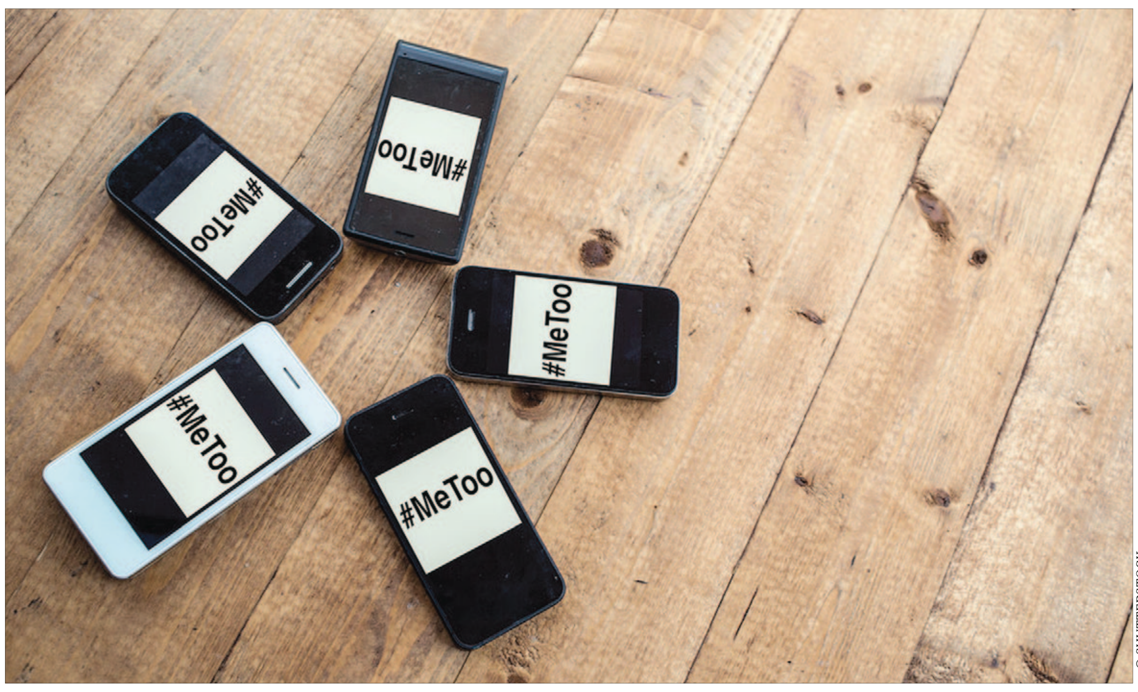
If the widely-reported allegations flowing from the #MeToo and #TimesUp movements weren't enough of a wake-up call for New York corporations, the New York Attorney General has issued a sharp warning about systemic workplace sexual harassment that all organizations doing business in New York state, and their principals, directors, managers and employees, would be wise to heed. On Feb. 11, 2018, the Attorney General filed a lawsuit against The Weinstein Company (TWC), its parent holding company, and co-owners Harvey and Robert Weinstein, alleging workplace sexual harassment that spanned more than a decade. Under the broad scope of New York Executive Law §63(12), the Attorney General brought claims of "repeated and persistent illegality," of which corporate management and directors were allegedly aware, but failed to adequately investigate or stop. With that filing, the Attorney General made clear that organizations doing business in New York now have much more to fear than private actions alleging sexual harassment. The Attorney General sent a strong message that companies and individuals that allow or foster workplace sexual harassment, fail to take adequate steps to prevent it in the first place, or fail to investigate and address complaints that are made, can incur severe consequences backed by the full investigative and enforcement power of the government. And, for organizations that wisely choose to be proactive in preventing workplace sexual harassment, the Attorney General's lawsuit provides a roadmap for implementing effective compliance programs and enhancing existing programs to ensure that their employees are not victimized by sexual harassment and that they and their principals, directors, managers and employees are not on the receiving end of similar Attorney General actions.

ROSS M. KRAMER *and* SUZANNE JAFFE BLOOM *are partners at Winston & Strawn.*

Attorney General's Allegations

In its lawsuit, the Office of the Attorney General (OAG) paints a picture of a systemic, company-wide culture of sexual harassment, perpetrated against women by one executive, but allegedly enabled, facilitated, and hidden for years by an assembly of managers, executives, and employees. According to the complaint, OAG brought action against Harvey and Robert Weinstein (as co-owners, co-chairmen of the board, and co-chief executive officers), The Weinstein Company, and its parent holding company, "to remedy a years-long gender based hostile work environment, a pattern of *quid pro quo* sexual harassment, and routine misuse of corporate resources for unlawful ends." The complaint makes clear that OAG filed its lawsuit in response to "repeated, persistent and egregious violations of law, to vindicate the rights of TWC's employees, and to prevent future recurrence of such misconduct."

According to the complaint, OAG initiated its investigation after learning of published reports that Harvey Weinstein used his role as co-CEO, and his power in the entertainment industry, to sexually harass and abuse numerous women. OAG also alleged that TWC not only knew about Weinstein's misconduct and failed to take adequate steps to protect employees, but also took affirmative steps to shield the harassment and abuse through, among other means, the aggressive use of non-disclosure agreements (NDAs), which prohibited settling complainants from disclosing their experiences and thereby concealed the underlying misconduct.



© SHUTTERSTOCK

With regard to Weinstein personally, OAG alleged that he "repeatedly and persistently" sexually harassed female employees at TWC by creating a hostile work environment that "pervaded the workplace," and by demanding that women engage in sexual or demeaning conduct "as a *quid pro quo* for continued employment or career advancement." Among other more salacious allegations (see, e.g., the allegation that TWC employees had to procure and administer Weinstein's "erectile dysfunction shots"), OAG claimed that Weinstein regularly subjected female TWC employees and interns, and women seeking job opportunities, to unwelcome, unwanted, and inappropriate physical and sexual contact and touching, leering, and a "barrage of gender-based obscenities" and "gendered insults," and that his persistent actions created a "toxic environment for women" at TWC. OAG also alleged that Weinstein made quid pro quo offers or demands of sexual favors of female employees and interns in exchange for career advancement at TWC, or to avoid adverse employment consequences.

With regard to TWC, OAG's complaint made clear that its allegations against the company were rooted in TWC's inaction and concealment of extensive evidence of persistent sexual harassment. OAG alleged that TWC bore corporate responsibility because of Weinstein's position at the company, because Weinstein used TWC's corporate resources and employees to facilitate his misconduct,

> The Attorney General's lawsuit provides a **roadmap for implementing effective compliance programs** and enhancing existing programs to ensure that their employees are not victimized by sexual harassment.

and because TWC "was aware of and acquiesced in repeated and persistent unlawful conduct" by failing to adequately investigate or stop it. OAG alleged that Weinstein's regular use of gender-based obscenity and insults was made in front of TWC employees, "including the company's most senior executives"; that "multiple groups" of TWC employees were actually tasked with facilitating his sexual encounters with women; and that despite its awareness of the problem, the company failed to take any institutional action to investigate allegations or to protect employees or interns from future misconduct.

Further, OAG alleged that TWC's management and Board of Directors "were repeatedly presented with credible evidence" of Weinstein's sexual harassment of employees and interns, and were "fully aware" of Weinstein's creation of a hostile work environment and sexual harassment, but failed to "investigate and discover the nature and extent of the misconduct," restrict Weinstein's ability to hire or supervise employees, or terminate his employment altogether. Similarly, OAG alleged that management "deliberately looked the other way," or took actions that enabled Weinstein to retaliate against employees who complained about his misconduct. OAG alleged that rather than investigate and take prompt corrective action, TWC "used settlements that contained strict NDAs to keep law enforcement, the public, and even other TWC employees from discovering the extensive allegations of misconduct." As a result, OAG alleged, TWC enabled Weinstein's unlawful conduct to continue "far beyond the date when, through reasonable diligence, it should have been stopped."

New York Executive Law §63(12) and the OAG Investigation

Under Executive Law §63(12), OAG is empowered to bring an action seeking injunctive relief, restitution, damages, disgorgement, civil penalties and costs, whenever any person (meaning individual or organization) has "engage[d] in repeated fraudulent or illegal acts or otherwise demonstrate[d] persistent fraud or illegality in the carrying on, conducting or transaction of business."

Section 63(12) is a purposefully broad statute, allowing OAG to investigate and take action against a wide range of businesses engaging in "repeated" or "persistent" illegality. Pursuant to §63(12), OAG "is authorized to take proof and make a determination of the relevant facts," and to issue subpoenas in accordance with the CPLR. OAG made use of its extensive authority under the law to investigate and ultimately bring charges here. According to the complaint, as part of its investigation OAG issued a subpoena to TWC and third parties for documents and testimony, and received "correspondence, business records, financial records, and thousands of pages of documents"; OAG also interviewed current and former employees, executives and Board members of TWC.

This is not the first time that OAG has employed §63(12) to investigate and charge organizations and individuals that have "engage[d] in repeated fraudulent or illegal acts or otherwise demonstrate[d] persistent fraud or illegality in the carrying on, conducting or transaction of business." Over the past decade, OAG has employed §63(12) against, among others: landlords who permit properties to be persistently used

» Page 15

© SHUTTERSTOCK

The End of the **Internal Investigation** and the Risk Of the **Internal Whistleblower**

BY REETUPARNA DUTTA AND MICHELLE MEROLA

The Foreign Corrupt Practices Act—the first law to outlaw bribing foreign officials—has two main prohibitions. The anti-bribery provisions prohibit the offering or payment of anything of value to foreign officials to influence their acts or decisions for the purposes of obtaining or retaining business. 15 U.S.C. §§78dd-1, 78dd-2, 78dd-3. The accounting provisions require that "issuers" (companies listed on a U.S. exchange or required to file reports with the SEC) keep records which "in reasonable detail" accurately and fairly reflect transactions and also maintain a system of internal accounting controls sufficient to provide "reasonable assurances" that transactions are authorized and recorded properly. 15 U.S.C. §78m(b)(2).

With respect to FCPA enforcement, the Trump Administration has followed in its predecessor's footsteps by mandating voluntary self-disclosure of violations to obtain leniency in prosecution and sentencing. Beginning in April 2016, the Department of Justice started a "Pilot Program" to incentivize companies to voluntarily self-disclose FCPA violations and cooperate with the government. See DOJ, The Fraud Section's Foreign Corrupt Practice Act Enforcement Plan and Guidance (April 5, 2016). In November 2017, Deputy Attorney General Rod Rosenstein announced a new FCPA Corporate Enforcement Policy that adopts the Pilot Program's emphasis on voluntary self-disclosure, cooperation and remediation. Specifically, when a company has voluntarily self-disclosed, cooperated, and remediated, it will receive a declination of prosecution absent certain aggravating factors, including involvement of high-level executives in the misconduct, a significant profit to the company from the misconduct, or the pervasiveness of the misconduct in the company. If criminal proceedings are warranted, the government will recommend a 50 percent reduction off the low end of the Sentencing Guidelines' fine range (except in the case of a recidivist company) and will not require the company to obtain a monitor, as long as the company has implemented an effective compliance program. In the absence of voluntary self-disclosure, and even assuming that the company has cooperated and appropriately remediated, the DOJ will only recommend a 25 percent reduction from the low end of the Guidelines' fine range. See DOJ, FCPA Corporate Enforcement Policy.

And self-disclosure is paying off. For example, in 2017, the DOJ declined to prosecute Linde North America and Linde Gas North America (collectively, Linde) and certain of their subsidiaries under the FCPA. The DOJ found that Linde, via a subsidiary, made corrupt payments to high-level officials at a state-owned and controlled entity in the Republic of Georgia. The DOJ declined prosecution based on Linde's timely and voluntary self-disclosure; its thorough and proactive investigation; its full cooperation; its agreement to disgorge the profits received from the improper conduct; the steps it took to enhance its compliance program and internal controls; and its full remediation, including disciplinary action. Letter from DOJ to Steptoe & Johnson (June 16, 2017).

But self-disclosure has to be quick for a declination. For example, also in 2017, Keppel Offshore & Marine, a Singapore company and its wholly-owned U.S. subsidiary, Keppel Offshore & Marine USA, agreed to pay approximately $422 million to resolve charges in the United States, Brazil, and Singapore arising from a scheme to pay bribes to Brazilian officials. The subsidiary and a former member of its legal department plead guilty to conspiracy to violate the FCPA, while the parent company entered into a deferred prosecution agreement pursuant to which it agreed to implement internal controls and cooperate with the DOJ. The DOJ noted that the companies received credit for their cooperation and remedial measures, which was reflected in a criminal penalty that was a 25 percent reduction off the bottom of the applicable Guidelines' fine range. Press Release, Keppel Offshore & Marine Ltd. And U.S. Based Subsidiary Agree to Pay $42 Million in Global Penalties to Resolve Foreign Bribery Case(Dec. 22, 2017). But there was no credit for voluntary self-disclosure because:

> [A]lthough [the company] notified the Fraud section about publicly-reported allegations in Brazil prior to the Fraud Section and the Office contacting the Company, the Fraud Section and the Office *were already aware of the allegations*.

United States v. Keppel Offshore & Marine, Case No. 17-cr-697, Deferred Prosecution Agreement, ¶ 4(a) (emphasis added); see also *United States v. Keppel Offshore & Marine USA*, Case No. 17-698, Plea Agreement, ¶ 2(b).

The government has enormous resources—both domestically and internationally—from which to glean information about potential violations. In a speech on Nov. 9, 2017, then-Acting Assistant Attorney General Kenneth A. Blanco highlighted the international cooperation that led to a number of high-profile FCPA prosecutions, including the prosecution of Odebrecht, one of the world's largest construction companies. The United States worked with Brazil and Switzerland to obtain the largest global fine ever imposed in a corruption case and, as AAG Blanco noted, they "assisted one another in gathering evidence and building the case." Acting Assistant Attorney General Kenneth A. Blanco Delivers Remarks at Foreign Corrupt Practices Act/Organization for Economic Cooperation and Development Anniversary Conference at the NYU School of Law (Nov. 9, 2017).

Another reason for quick self-disclosure is the risk of whistleblowers. The SEC, which has civil enforcement authority over the FCPA with respect to issuers, has a whistleblower program where individuals who voluntarily provide it with original information relating to the violation of securities laws (which include the FCPA) can obtain a portion of a successful recovery. And the importance of whistleblowers to the government is illustrated by recoveries under the False Claims Act, which provides a portion of any recovery to whistleblowers who initiate actions on behalf of the government for fraud. In 2017, the government recovered $3.4 billion as a result of whistleblower lawsuits under the False Claims Act and paid out $392 million to whistleblowers. Press Release, Justice Department Recovers Over $3.7 Billion from False Claims Act Cases in Fiscal Year 2017.

But beyond the monetary rewards, many employees may still "blow the whistle." A survey of False Claims Act whistleblowers found that their motivations "coalesced around four non-mutually exclusive themes: integrity, altruism or public safety, justice, and self-preservation." Aaron S. Kesselheim, et al., "Whistle-Blowers' Experiences in Fraud Litigation against Pharmaceutical Companies," The New England Journal of Medicine (May 13, 2010). When monetary incentives are combined with ethical dilemmas and concerns over liability, there is a significant risk that a company employee will disclose misconduct to the government before the company has the chance to do so.

> Companies that wait to discover potential misconduct and then conduct a thorough and comprehensive internal investigation before taking remedial action will **likely lose out on substantial benefits**, including possible declination of prosecution.

Where time is of the essence, the traditional model of internal investigations cannot survive. While engaging outside counsel is necessary, reviewing scores of documents, conducting witness interviews, and coming up with a deliberative strategy to disclose misconduct will risk missing out on self-disclosure benefits. Internal investigations will have to become streamlined, and companies will have to consider disclosing potentially improper conduct even before reaching a definitive conclusion as to its illegality. Indeed, the true internal investigation may come *after* self-disclosure and pursuant to the directive of the government, as the company works with the government to identify the misconduct and the culpable individuals. For example, in the Keppel prosecution, the government gave Keppel credit for its "substantial cooperation" with the government, which included

> [C]onducting a thorough internal investigation, meeting the Fraud Section's and the Office's requests promptly, proactively identifying issues and facts that would likely be of interest to the Fraud Section and the Office, making regular factual presentations to the Fraud Section and the Office, agreeing to make foreign-based employ-

» Page 15

REETUPARNA DUTTA *and* MICHELLE MEROLA *are partners at Hodgson Russ.*

The **Sea Change Across the Pond:** UK Privilege In Internal Investigations Remains in Flux

BY ROGER A. BURLINGAME,
STEVEN G. KOBRE
AND RACHEL E. GOLDSTEIN

Following a series of English High Court decisions that upended standard practice for lawyers conducting internal investigations in the UK, a recent ruling suggests the British assault on privilege may be reaching its end, but the bounds of protection remain unclear.

Starting with 2016's *In re RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch) (*RBS*) and continuing through last year's *Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd* [2017] EWHC 1017 (*ENRC*), the English High Court dramatically limited privilege protections in the context of internal investigations. Taken together, the decisions held that English legal advice and litigation privileges frequently do not protect attorney notes and interview memoranda generated in UK-based internal investigations, allowing disclosure of such materials to both private litigants and UK prosecutors.

Where *RBS* and *ENRC* raised alarm among practitioners, the recently decided *Bilta (UK) Ltd v. Royal Bank of Scotland* [2017] EWCH 3535 (Ch) (*Bilta*) offers hope. The decision sets limits on the principles articulated in *ENRC* and gives crucial guidance for attorneys seeking to protect their investigative materials. It does not, however, overrule its predecessors, and significant uncertainty about the scope of privilege in the investigations context remains.

Litigation Privilege

The British recognize two forms of legal professional privilege. Legal advice privilege protects written or oral communications between attorney and client generated for the purpose of providing or seeking legal advice. Litigation privilege provides broader protections, encompassing communications between attorney and client as well as third parties, but only when (1) the litigation is "in progress or in contemplation"; (2) the communications are made "for the sole or dominant purpose of conducting that litigation"; and (3) the litigation is "adversarial, not investigative or inquisitorial." *ThreeRivers District Council v. Governor & Company of the Bank of England (No 6)* [2005] 1 AC 610.

In *ENRC*, the High Court held that litigation privilege did not protect materials generated by ENRC's outside solicitors and accountants during an internal investigation that kicked off in response to an anticipated criminal investigation by the UK's Serious Fraud Office (SFO). In rejecting ENRC's privilege claim, the court held that:

• *Reasonable anticipation of a criminal investigation did not equate to reasonable contemplation of litigation (a prosecution).* Finding that the litigation privilege applies solely to materials generated when the company reasonably contemplates a prosecution, the court found that ENRC needed a factual basis to expect that the prosecutor could secure a conviction before it could claim privilege. The mere likelihood (or existence) of the investigation was not enough.

• *Documents created for the purpose of responding to the investigation or dissuading prosecutors from bringing charges were not made for the "dominant purpose" of conducting litigation.* To satisfy the second prong, the court held that materials must be created for the purpose of conducting a defense to a prosecution.

• *Discussions with the prosecutor during an investigation were not "adversarial litigation."* Even an investigation conducted under a well-grounded fear of a criminal investigation did not qualify as "adversarial litigation."

ENRC created a conundrum. In its wake, privilege attaches to an internal investigation responding to a criminal investigation only when the company determines there is enough "truth in the accusations" to make prosecution "a real prospect." But to get to that stage, of course, the company must investigate without privilege protection.

'Bilta' Pushes Back

Limiting its holding in *ENRC*, the High Court in *Bilta* ruled that, under certain circumstances, litigation privilege can apply to documents generated in this context.

In *Bilta*, liquidators suing the Royal Bank of Scotland (RBS) for fraud sought discovery of documents created by RBS' solicitors in an internal investigation triggered when Her Majesty's Revenue and Customs (HMRC) sent a letter (1) alleging that RBS' participation in fraudulent transactions created fraudulent tax claims, and (2) permitting RBS to respond before HMRC made its assessment. Relying on *ENRC*, Bilta argued that privilege did not apply because the investigation was not undertaken for the dominant purpose of conducting litigation, but rather to inform RBS of its exposure to the allegations, to cooperate with HMRC, and to convince HMRC not to issue an assessment.

Rejecting these arguments, the court found that the approach taken in *ENRC* could not be applied to all scenarios involving companies conducting investigations in the shadow of a prosecutorial or regulatory action. Instead, it emphasized that courts should "take a realistic, indeed commercial, view of the facts" when assessing the sole or dominant purpose of an investigation.

In further contrast to *ENRC*, in *Bilta* the court held that where investigations have multiple purposes, the privilege could apply, provided litigation is the dominant purpose. (The court recognized that preparing for litigation can subsume the "inseparable purpose" of avoiding litigation.)

> Where 'RBS' and 'ENRC' raised alarm among practitioners, **the recently decided 'Bilta (UK) Ltd v. Royal Bank of Scotland' offers hope.**

Based on its analysis of the commercial reality of RBS' situation, the court concluded that its investigation's dominant purpose was to defeat the litigation that would follow HMRC's "almost inevitable" assessment. The holding hinged on the following findings:

• The HMRC letter was a "watershed moment": It cited sufficient evidence for an assessment and gave RBS reason to believe it was highly likely that an assessment would follow. The letter thus signified a shift from an investigation to a tax dispute, making it unlikely that RBS' response to the letter would dissuade HMRC from issuing an assessment.

• RBS' decision to retain external solicitors with expertise in tax litigation to help lead the investigation "strongly suggest[ed]" that it contemplated an assessment and was preparing to defend a claim.

• Other evidence also showed that RBS' lead officials considered it highly likely that an assessment would be issued.

• RBS' "ostensibly collaborative and cooperative" interactions with HMRC after receipt of the letter—including RBS' submission of a report detailing why HMRC should not make an assessment—did not preclude it from being conducted for the dominant purpose of litigation.

In sum, the court concluded that the "commercial reality" was that RBS' internal protocols and statutory obligations compelled it to cooperate with HMRC despite RBS' knowledge that there was an "overwhelming probability" HMRC would make an assessment. In that context, the report was consistent with the "overarching purpose" of preparing for litigation to challenge the assessment.

In contrast to *ENRC*, where efforts to settle the litigation precluded a finding that litigation was the dominant purpose, the *Bilta* court held that a comprehensive view of the facts in light of the company's commercial reality compelled a finding that RBS would not have made such significant expenditures on legal fees in the hopes of dissuading HMRC from issuing an "almost inevitable" assessment, but rather did so for the primary purpose of preparing a robust defense.

The Path Forward

The tension between *ENRC* and *Bilta* will remain at least until the Court of Appeals decides *ENRC*'s appeal (scheduled for hearing in July 2018). In the meantime, taken together the two cases suggest a number of best practices for attorneys looking to protect materials generated during a UK internal investigation:

• Before commencing an internal investigation—particularly concerning allegations with potential criminal exposure—attorneys should preliminarily assess whether litigation is in reasonable contemplation. If it is, attorneys should consider documenting the bases for this conclusion, detailing the context that create a fear of prosecution.

• Retain external legal counsel with a specialty in the subject matter of the litigation to help manage the investigation. The engagement letter should describe the scope of work in light of the purpose to defend against the anticipated claims, supporting a finding that the dominant purpose of the investigation was to prepare a defense.

• After commencing an investigation, attorneys and other personnel should keep clear records of the purpose of the investigation and the circumstances that prompted it, including records of any correspondence with potential adversaries or other evidence that reflects a strong probability that litigation will ensue.

• Absent a well-documented and objective expectation that litigation is highly probable, documents created for the purpose of settling or discouraging a regulator from initiating litigation, or advising the client on how best to avoid litigation, may preclude a finding that litigation is the dominant purpose. Accordingly, attorneys drafting such materials should do so with the knowledge that if resolution is deemed a primary goal of the investigation, protection may be lost.

While *Bilta* suggests the High Court may have pulled back from the most troubling aspects of *ENRC*, unless and until the UK's Court of Appeals weighs in, practitioners should consider the above, understanding that materials unquestionably deemed privileged in the U.S. could well garner no such protection in the UK.

ROGER A. BURLINGAME, STEVEN G. KOBRE *and* RACHEL E. GOLDSTEIN *are lawyers at Kobre & Kim.*

© SHUTTERSTOCK

Health Care

« Continued from page 11

matively prove this process was actually used.

(5) Kickbacks. The payment of kickbacks or other illicit benefits to patients, recruiters who procure such patients, or even to doctors or other medical professionals, continues to be a major problem. Where appropriate, clinics should actively question management as to how the patients learned of the clinic or why the patient selected your clinic over others. Your internal data will show if the patient is a "frequent flier" in your office and whether the patient has presented with a number of different ailments over time that seem implausible or has received treatment at your facility for which they inexplicably re-present multiple times. This could be suggestive of a patient who is being paid to visit your facility. If one patient is being paid, it is likely there are more. Criminal penalties for paying and receiving kickbacks are severe, and any suggestion that this is occurring should be investigated immediately.

(6) Upcoding. Upcoding refers to the improper practice of a medical professional billing for a more expensive medical service than was actually provided to the patient. While upcoding can occur in a myriad of ways, DOJ often focuses on service-based, location-based or time-based upcoding. In service-based upcoding, a doctor may perform a simple check-up, but bill for a more extensive examination or even a surgery. A location-based example could be billing for a procedure that occurred in an operating room when, in fact, it had occurred in a less-expensive setting such as an office. Finally, time-based upcoding fraud can occur when a doctor sees a patient for 10 minutes, but bills for a more expensive 45-minute consultation. These upcoding schemes are more difficult for law enforcement to unravel, but the claims data will give rise to greater potential scrutiny when providers consistently use higher-paying codes.

> Make no mistake—federal enforcement of criminal health care laws stands poised to become **increasingly muscular and robust.**

(7) Billing for Unqualified Workers. Another common theme in health care fraud cases is billing for unqualified or unlicensed workers. On the obvious side, many cases have featured clinics using a less qualified worker (such as a physician's assistant) to render services to a patient, but the services are billed as if they were provided by a medical professional with a higher reimbursement rate. Other subtler variations on this theme are clinics that bill for lower-level medical professionals (such as physical therapy assistants) who are supposed to be supervised by a higher-level medical professional (a physical therapist) but operate without supervision. Your facility must have the proper monitoring equipment (e.g., electronic badging, timecards, etc.) to be able to demonstrate which medical professional actually saw the patient and in the case of supervision requirements, who was on-site when certain care requiring supervision was rendered.

Conclusion

The administration has backed up its tough talk on combating health care fraud with new initiatives and more money. Make no mistake—federal enforcement of criminal health care laws stands poised to become increasingly muscular and robust. Knowing the red flags the federal authorities will look for will help your company be more compliant and mitigate the risk of becoming the subject of a federal criminal health care fraud investigation.

Sanctions

« Continued from page 11

face liability for even unintentional violations. Given the high stakes all around, one might expect an abundance of data proving the effectiveness of sanctions programs that have been administered by OFAC since 1950. However, this does not appear to be the case. See *Examining the Effectiveness of the Kingpin Designation Act in the Western Hemisphere: Hearing Before the H. Comm. on Foreign Affairs, Subcomm. on the W. Hemisphere*, 115th Cong. 2 (2017) (statement of Eric L. Olson, Deputy Director, Latin American Program, Senior Advisor, Mexico Institute, Woodrow Wilson International Center for Scholars: Witness unaware of any public report or comprehensive review of the effectiveness of the program and policy behind the Foreign Narcotics Kingpin Sanctions Regulations).

In 2001, the Judicial Review Commission on Foreign Assets Control conducted a limited review of OFAC sanctions programs under a directive to examine the constitutionality of the Kingpin Act. The Commission submitted a report to Congress recommending that Congress amend licensing procedures to be more responsive to the legitimate needs of U.S. persons affected by blocking actions; that OFAC promulgate regulations to establish "safe harbors"; and that OFAC establish a dialogue with the U.S. business community affected by sanctions laws. These recommendations have not been implemented. *Administrative History Note*, Judicial Review Commission on Foreign Asset Control, Organization Authority Records, National Archives. The failure to address these recommendations represents a lost opportunity to measure the costs and benefits of sanctions programs.

OFAC Undeterred

Notwithstanding the absence of data in its favor, OFAC asks more and more of its private-sector gatekeepers. OFAC administers 28 active sanctions programs that have continually grown, targeting specific industries and activities, while at the same time becoming more expansive. This growth places increasingly costly compliance burdens on U.S. businesses. And the costs are enormous, as much as billions of dollars per year. See, e.g., Hui Chen & Eugene Soltes, "Why Compliance Programs Fail—and How to Fix Them," Harvard Business Review (March-April 2018); "Uncovering the True Cost of Anti-Money Laundering & KYC Compliance," A LexisNexis Risk Solutions Report Study on Financial Institutions Across Six Markets in Asia (2016); Laura Noonan, "Banks Face Regulatory Pushback over Surging Compliance and Regulatory Costs," Financial Times (May 28, 2015).

> Is the cost to U.S. business justified by the benefits of sanctions? In other words, are **U.S. economic sanctions programs** effective in achieving their stated goals?

From a national security perspective, this burden might make theoretical sense. The problem is the absence of concrete data justifying the burden by showing that sanctions actually improve national security. In light of this absence of data, shouldn't some consideration be given to the question of how much of a burden businesses should be asked to bear?

Apparently not. In addition to increasing the breadth and depth of its sanctions programs, OFAC has further increased the burden on businesses by means of an agency rule known as the 50 Percent Rule. Under this rule, U.S. businesses are required to determine whether any potential transaction involves entities owned 50 percent or more by a blocked party—even if the blocked party itself is not otherwise involved in the transaction. In other words, OFAC requires U.S. businesses to ferret out the hidden entities and block transactions with them even where OFAC has not been able to detect and sanction those entities. OFAC's justification for the 50 Percent Rule is that sanctioned individuals—particularly sophisticated ones—often hide behind front companies with complex and anonymous ownership structures. This is no doubt true. But shouldn't OFAC be the one to identify entities hiding behind front companies? If OFAC can't figure it out, why should this investigative burden shift to private businesses, particularly small ones?

While the 50 Percent Rule might make theoretical sense to the government, as a practical matter, most businesses do not have the resources to uncover the ownership structures of all their customers and business partners. Even large multinational institutions struggle to appropriately integrate compliance practices that identify beneficial ownership and properly screen upstream owners.

In 2014, OFAC issued its first (and to date, only) penalty for a violation of the 50 Percent Rule. Barclays Bank Plc (Barclays), a financial institution headquartered in the United Kingdom, agreed to pay nearly $2.5 million to settle potential violations for processing transactions of subsidiaries owned 50 Percent or more by an SDN. See OFAC Enforcement Information for Feb. 8, 2016.

What Can Be Done?

Even in the absence of any data driven justification for OFAC's sanctions, the programs are here to stay. So too, likely, is the 50 Percent Rule. Thus, businesses will continue to face compliance challenges including whether to expend substantial resources trying to identify upstream ownership of their customers—or risk hefty OFAC penalties for inadvertent violations.

We recommend that OFAC empirically examine the effectiveness of its programs, with a particular focus on the 50 Percent Rule. If, as the authors suspect, the results show that the 50 Percent Rule places a greater burden on U.S. business than is justified by the result, then OFAC should abandon the rule and create a safe harbor for businesses that act in good faith to comply with OFAC sanctions programs. In the end, the duty to protect the national security belongs to the government and is not delegable. The government, with its national security mandate, is in the best position to identify entities that pose a threat, and should, therefore, reclaim responsibility for sanctioning those entities.

‘Glassdoor’

« Continued from page 11

taken in bad faith. Glassdoor had argued that the *Branzburg* “bad faith” test was inapposite, insisting that the Ninth Circuit’s holding in *Bursey v. United States*, 466 F.2d 1059 (9th Cir. 1972), set a stricter standard of review.

Which precedent should control was again the battleground on appeal. Glassdoor argued that the rights of anonymous *speakers*, see *McIntyre v. Ohio Elections Commission*, 514 U.S. 335 (1995), were distinct from the reporter’s privilege claims in *Branzburg*. They urged instead that *Bursey*’s three-part test controlled, requiring an immediate and substantial interest of the government in the information; a substantial connection between the information and that interest; and the least drastic means necessary to secure it. *Bursey*, 466 F.2d at 1083.

The panel rejected Glassdoor’s *Branzburg* analysis as a “distinction without a difference,” noting that the Supreme Court had there addressed the argument that an inability on the part of journalists to safeguard confidential sources would deter reluctant speakers, compromising the free flow of information. Thus Glassdoor, a forum for anonymous speech and would-be guarantor of that anonymity, echoed the *Branzburg* journalists. The panel also emphasized that the site’s anonymous-use policy had caveats. Users were required to certify their acceptance of Glassdoor’s terms, including a “Privacy Policy” qualifying its general non-disclosure to permit compliance with “relevant laws ... subpoenas ... or legal process[.]” (The Circuit also disagreed that enforcing the subpoena would infringe users’ “associational privacy,” reasoning that the website, comprising anonymous commentary among participants unknown to one another, did not implicate the “expressive association” protected by *NAACP v. Alabama*, 357 U.S. 449 (1958).)

Takeaways

The scope of this article cannot fully digest the serious issues implicated, and readers should review the panel opinion and briefing, including amici curiae submissions by Electronic Frontier Foundation and others. A few observations about the panel’s approach:

Terms of use disclaimers inconsistent with absolute anonymity. Speech advocates fairly complain that the practicalities of online forums require some identification for the user to participate. The panel stressed this pedigree data, and the site’s disclaimer about response to legal process, to question whether users had an absolute expectation of privacy. Although such “fine print” could be seen as expanding compelled disclosure, Glassdoor did fight the good fight for its users here, and intrusions on anonymity should still be exceedingly rare. Civil subpoenas, for instance, would not benefit from the *Branzburg* analysis employed. (Moreover, though it may be small comfort to advocates, Rule 6(e) grand jury secrecy might still conceal from the public the identity of speakers approached by investigators.)

‘Branzburg’ and ‘Bursey’ analysis perhaps not that different. Although the panel came down in favor of *Branzburg* and the government, it stated that it would have reached the same outcome under *Bursey*. The latter case involved a probe of the Black Panthers newspaper, related to alleged threats against President Nixon. The investigators’ transgression there was in the second *Bursey* prong—the lack of a “substantial connection” between the legitimate interest in investigating threats and the political subjects actually scrutinized. That disconnect was the constitutional grievance, and it is hard to distinguish that intrusion from the “bad faith” exception recognized in *Branzburg*. Under either approach, deference to grand juries would seem to extend only to genuine pursuit of criminal evidence.

No ultimate privilege against users’ testimony. The panel noted in its *Branzburg* analysis that the court declined to create a “privilege” for reporters to avoid a grand jury where the protected sources themselves would enjoy no such privilege—the Fifth Amendment being the only exception to the rule that the public has a right to every citizen’s evidence. This would seem to be the sticking point in any confidentiality confrontation. If a potential witness possesses evidence owed the public, and there is a means to compel appearance, no intervening claim of privilege (other than self-incrimination) will likely prevail.

> Although litigation over anonymous online speakers is unlikely to be settled by this controversy alone, there are reasons to expect (or hope) that prosecutors will pursue other avenues to locate persons with knowledge of corporate fraud.

To Cast a Wide Net?

That the *Glassdoor* panel endorsed the government’s request for users’ identities—at least as to the shorter list of eight—is not surprising. Courts do defer to grand jury investigations, and absent truly intrusive overreaching motions to quash will seldom prevail. What would be at risk in civil litigation of rejection by a court as a “fishing expedition” will often merit enforcement through the grand jury, because of the clear societal interest in investigating potential crimes. The interesting question posed by scenarios like *Glassdoor*, then, may not be whether the government can go fishing, but whether it should. With apologies to Matthew’s Gospel, a broad subpoena for unknown persons will make prosecutors “fishers of men,” and there are reasons to consider what kind of catch you might pull before you put your net in the water.

Anonymity can be a powerful catalyst for truth, but it can also be a haven for exaggeration, vindictiveness and outright falsehood. In the employment context, the urge to “flame” the company can be considerable and, on the nameless Internet, usually without consequence. Anonymous commentators who exaggerate or invent wrongdoing can create headaches for the government when approached by agents. If one lies, and defends his inaccurate posting, he has not only misled investigators but likely committed a crime that could explode in his face (and the government’s case). If one tells the truth, and backs away from overheated accusations to deny fraud, her account could well be exculpatory material subject to disclosure under the *Brady* doctrine. Some posts would be accurate and corroborated, but the bigger the net the greater the risk, and the potential problems are both serious and avoidable.

As tempting as it might be to pursue sources of unsigned posts, the government already has the ability to survey employees from whom such comments would have come. With organizational charts and employee lists, and assisted by company counsel, prosecutors can identify persons with knowledge. Represented by counsel in interviews, employees should be well prepared to give coherent, truthful accounts of whatever they know. A meeting in a prosecutor’s office is an experience most will take seriously; a visit to the internet may not be.

It is also worth remembering that a worthy insider witness—an organized thinker who wants to do the right thing—should have the wherewithal to contact the government if so motivated. Statutory incentives like the False Claims Act will attract some, but the larger question is whether it makes sense to pursue a source who sounds an “alarm” without stepping forward. (In negotiations preceding its motion Glassdoor apparently made some offer to contact users to explore voluntary cooperation, but the prosecutors declined. That is perhaps understandable, but such compromise merits consideration. Except where the information implicates physical safety, it is difficult to see any real return in chasing non-volunteers, and reticence may have its reasons.)

Conclusion

Online speech is abundant and often unattributed. The *Glassdoor* ruling suggests that where content hints at knowledge of criminality investigators will be permitted to track its sources. The temptation to peel back the cover is obvious, but heedfulness is warranted—to avoid chilling salutary speech, and to escape grief from the more mischievous kind.

Warning

« Continued from page 12

for criminal activities, as part of OAG’s “Nowhere to Hide” program; an individual and management company who invested client funds with Bernard Madoff, for a pattern of fraudulent concealment and misrepresentation; real estate developers who raided a reserve fund meant to ensure the health and safety of tenants, for persistent fraud and illegality in the conduct of their business; a nationwide talent agency, for repeatedly misleading consumers through deceptive advertising; auto dealerships, for persistent fraudulent, deceptive and illegal business practices in the sale and financing of automobiles that left some consumers with ruined credit reports; and a major hospitality company for failing to provide consumers with timely notice that thousands of credit card numbers were exposed in security breaches, and failing to maintain reasonable data security, for deceptive acts and practices in conducting business.

The Weinstein lawsuit, however, represents a shift in focus for OAG under §63(12). The alleged misconduct—persistent illegality through workplace sexual harassment—fits squarely under the statute, but had not historically been a subject for OAG action under §63(12), until now. Rather than relying on laws prohibiting fraud as the predicates, OAG in this case looked to provisions of New York State Human Rights Law, New York City Human Rights Law, New York Civil Rights Law, and relevant provisions of the New York Penal Law to support its allegations. Ultimately, OAG asserted that Harvey and Robert Weinstein and TWC had “engaged in multiple, repeated and persistent” violations of §63(12), arising out of a decade-long pattern of systemic sexual harassment, by violating each of these underlying laws.

The Lessons of ‘People v. Weinstein’

OAG’s detailed allegations in this case provide both a warning and a roadmap for organizations to take significant steps to prevent workplace sexual harassment in the first instance, and to address all allegations and evidence of such harassment promptly, effectively and thoroughly. Organizations would be wise to act responsibly and proactively by implementing effective compliance programs, enhancing existing compliance programs, and taking preemptive steps to reform compliance procedures that may fall short.

The lessons and warnings of the *People v. Weinstein* case are myriad, but some stand out:

Having policies in place is simply not enough; those policies must have teeth and be visibly and regularly enforced by well-trained managers to demonstrate a company’s compliance in word and in practice. As alleged in the complaint, although TWC had a corporate policy prohibiting sexual harassment and discrimination, that policy was “flouted in practice.” Employees, including supervisors, who should have had reporting responsibilities, were alleged to have received no training or guidance about the company’s sexual harassment and discrimination policies, including how to report or handle a complaint.

> You must act responsibly, proactively, and decisively to prevent and address workplace sexual harassment, or you may face strong enforcement action and punishment by the state of New York.

An organization must have a Human Resources team entrusted and empowered to act on confidential complaints. That Human Resources team must also be able to act on complaints independently from the managers and executives who may be the subject of those complaints. OAG alleged that complaints directed to TWC Human Resources were often not treated confidentially, nor investigated. OAG alleged that the TWC Human Resources Director, who had the authority to investigate complaints, simply passed complaints along to the company’s COO without any further involvement in the investigation or resolution process. Further, OAG alleged that notwithstanding the authority to do so, “on not a single occasion” did the Human Resources Director start a formal investigation or implement any adverse employment consequences in response to a complaint about Weinstein’s behavior.

Organizations must have managers and Board Members who are ready, willing, and empowered to take action against individual bad actors, no matter what corporate title or power that person may hold. OAG’s complaint alleged that members of TWC management had knowledge of Weinstein’s misconduct toward women—from personal observations and from complaints that were filed—but failed to take action against Weinstein “due to his power within the company and his perceived importance to the company’s financial results.” OAG alleged that TWC’s Board likewise failed to adequately investigate, or prevent, Weinstein’s repeated misconduct. This was allegedly due in part to Harvey and Robert Weinstein’s influence over the Board, and in part to the Board’s concerns that Weinstein’s removal, or exposure of his misconduct, would risk financial harm to the company. OAG stated that the Board’s failure to investigate Weinstein’s misconduct, and the actions taken to shield Weinstein from any consequences for his misconduct, “enabled [him] to continue victimizing employees of TWC.” Notably, while mere inaction is on its own problematic, the TWC Board and management is alleged to have gone much farther than mere inaction, actively taking steps to shield Weinstein’s conduct by entering into NDAs with settling complainants.

In the end, any fears that TWC managers and Board members may have had about the damage that could result if they took action against Weinstein were dwarfed not only by the reported extensive harm suffered by the victims of his sexual harassment, but also by the financial and reputational damage to the company. The message of *People v. Weinstein* to organizations and their principals, directors, managers and employees is clear: You must act responsibly, proactively, and decisively to prevent and address workplace sexual harassment, or you may face strong enforcement action and punishment by the state of New York.

FCPA

« Continued from page 13

> ees available for interviews in the United States, producing documents to the Fraud Section and the Office from foreign countries ... and collecting, analyzing, and organizing voluminous evidence and information for the Fraud Section and the Office.

KOM Deferred Prosecution Agreement, ¶ 4(b).

But, while internal investigations may decrease in importance, companies must ensure that potential misconduct gets to their attention quickly so that they can self-disclose. Strong compliance programs are important in this regard, and companies should also consider incentivizing internal whistleblowers to report misconduct.

Encouraging a whistle-blowing culture, where employees feel safe and appreciated for disclosing what they believe to be improper conduct, is key. Fear of being ridiculed, ignored, or being subject to adverse actions chills many employees from coming forward with their concerns. But an environment where disclosure is rewarded (whether suspicions are validated or not) via a bonus, recognition, or even increased responsibility, may mean the difference between self-disclosing in time or missing out on those benefits.

Simply, quick self-disclosure is imperative. Companies that wait to discover potential misconduct and then conduct a thorough and comprehensive internal investigation before taking remedial action will likely lose out on substantial benefits, including possible declination of prosecution. Getting in front of the government early—even in the absence of certainty—may reap substantial benefits. And incentivizing insiders to “whistleblower” internally could help ensure that misconduct is discovered quickly so that the option to self-disclose still exists.