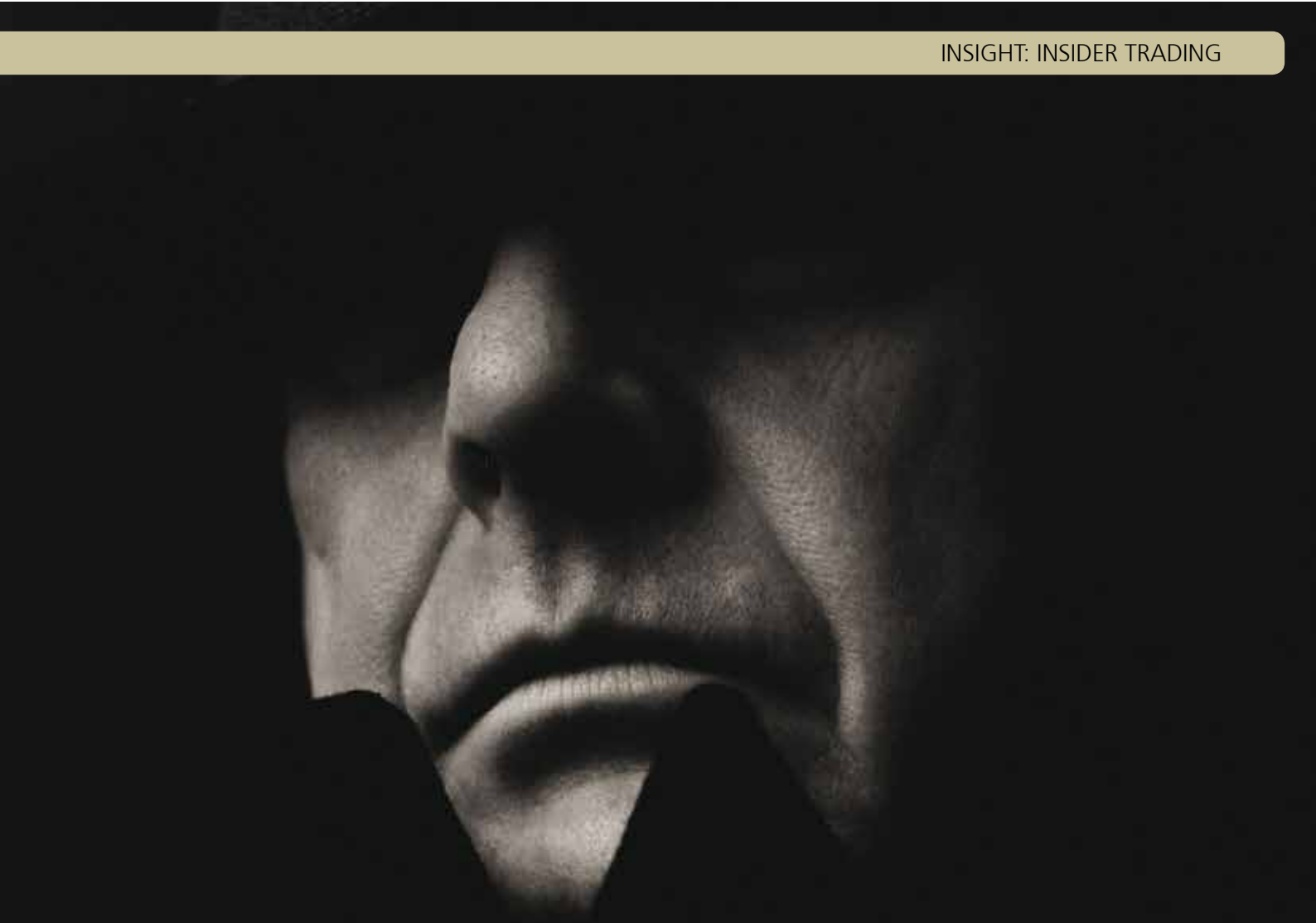

Keeping a watchful eye...

J.P. Hanlon, Kevin Kimmerling and **Michael MacPhail** explain how the FBI's ongoing crackdown on insider trading in the US is raising the stakes for regulated firms

Operation "Perfect Hedge", a US government investigation into insider trading activity, has resulted in more than 60 convictions in recent years. The investigation is unprecedented both in its scope and the use of aggressive prosecutorial tactics, such as covert wiretaps and cooperating witnesses, to reach individuals in the upper echelons of corporate America. While the criminal convictions in Perfect Hedge have been against individuals, the consequences at the organisational level have been substantial, and in some cases catastrophic.

What does this mean for compliance professionals? Most importantly, insider trading activity creates significant risk for the entities that employ or are affiliated with the individuals who engage in this prohibited conduct. With the aggressive investigation and prosecution of insider trading expected to continue for the foreseeable future, now is the time to reevaluate whether your organisation's compliance programme is effective in preventing and detecting insider trading as well as other potentially illegal activity.

"A stunning portrait of organised corruption on a broad scale"[1]

These words were used by Preet Bharara, the US Attorney for the Southern District of New York, recently included in *Time* magazine's list of the top 100 most influential people in the world[2], to describe the conduct of four investment professionals, including a co-founder of Level Global and a former portfolio manager at Diamondback. Bharara further explained that "Today's charges illustrate something that should disturb all of us: they show that insider trading activity in recent times has, indeed, been rampant and routine and that this criminal behaviour was known, encouraged and exploited by authority figures in several investment funds."[3]

When announcing the earlier, 2009, insider trading indictment of Galleon's Raj Rajaratnam, Bharara explained that, in "targeting white collar insider trading rings" the government today is using "the same powerful investigative tools that have worked so successfully against the mob and drug cartels."[4] These tools, including wiretaps, surveillance, and consensually recorded conversations, have proven extremely effective in persuading targets to plead guilty and juries to convict. More than 60 hedge fund traders, analysts, and industry consultants have been convicted.[5] And so far, the government has a perfect record at trial.[6]

This may be in part because wire-tapped conversations give jurors a contemporaneous glimpse into the complex world of trading and the mind of the accused. In the case of Raj Rajaratnam, the government played 45 wire-tapped conversations at his criminal trial.[7] Rajaratman was convicted, receiving an 11-year sentence, the second-longest ever for insider trading. A civil penalty of $92.8m, the largest ever, was eventually imposed against him.[8]

This is not to say that all insider trading cases in the future will necessarily involve wiretapped and consensually recorded conversations.[9] Due to limitations inherent in its role as an exclusively civil law enforcement agency, the Securities and Exchange Commission (SEC) cannot obtain wiretaps in the way the federal criminal authorities can. But even if the government is not "listening in", circumstantial evidence can still form the basis of insider trading charges. Take, for example, the case of John Michael Bennett and Scott Allen. The SEC alleged that Bennett paid Allen for inside information. Although the SEC had no recorded conversations describing such payments, the SEC alleged "on four separate days that Bennett withdrew $5,000 or more of cash from his bank accounts, Bennett and Allen swiped their Metrocards at the 59 Street Columbus Circle subway stop at the exact same time."[10]

An ounce of prevention

The Diamondback case illustrates the impact on organisations of insider dealing. Three employees of Diamondback Capital Management LLC, a hedge fund advisory firm, were convicted of insider trading activity. Diamondback appears to have done everything right in responding to the scandal: it turned over the results of its internal investigation to federal investigators, analysed trading patterns to determine suspicious trading activity, and otherwise cooperated with the authorities.[11]

Apparently acting in accordance with well-established policies giving "cooperation credit" to organisations that provide it with substantial assistance,[12] the SEC agreed to limit the fine imposed against the firm to $3m, an amount representing one-half of the $6m of allegedly ill-gotten trading profits.[13] obtained by the firm through insider trades on its behalf, whereas US law allowed the agency to seek penalties up to the amount of any illegal trading profits. In so doing, the SEC explained that it was giving "due credit to Diamondback for its substantial assistance in the government's investigation."[14]

For its part, the US Attorney's Office agreed not to prosecute Diamondback, lauding the firm for its "prompt and voluntary cooperation upon becoming aware of the government's investigation,"[15] and acknowledging that the firm's founders were unaware of the illegal conduct.[16]

But while Diamondback was rewarded for its efforts, the damage inflicted to its reputation was fatal. Diamondback, despite avoiding the "worst-case" scenario possible under the law, such as a criminal indictment and/or maximum monetary penalties, closed up shop after investors withdrew $520m (26% of its total assets).[17] The lesson is that compliance professionals must make preventing, as well as appropriately responding to, insider trading activity a top priority. In today's enforcement climate, however, encouraging employees to use internal procedures can be particularly difficult.

The incentive to cooperate

Government statutes and policies create powerful incentives for individuals to bypass internal procedures and report information regarding insider trading directly to the government. In the face of insider trading risks, the perceived benefit of "self-reporting" presents a particular hazard for compliance personnel. This is because employees involved in potentially illegal conduct have huge incentives to disclose their knowledge to government investigators without involving their employer, making a proactive response by the company more difficult. Employees ensnared in an SEC insider trading investigation may be advised to avail themselves of the agency's relatively >>

IN Brief:

- The US government's aggressive investigation and prosecution of insider trading is expected to continue.
- Insider trading activity creates significant risk for the entities that employ or are affiliated with individuals who engage in this prohibited conduct.
- There are powerful incentives for individuals to bypass internal procedures and report information regarding insider trading directly to the government.
- Preventing and detecting insider trading activity are critical components of an effective compliance policy.

> *"With the aggressive investigation and prosecution of insider trading expected to continue for the foreseeable future, now is the time to reevaluate whether your organisation's compliance programme is effective in preventing and detecting insider trading as well as other potentially illegal activity"*

new cooperation tools, which include formal cooperation, deferred prosecution and non-prosecution agreements based on, among other things, "[t]he assistance provided by the cooperating individual."[18] For example, on 19 March 2012, the SEC announced that it had credited the substantial cooperation of a former senior executive of an investment adviser in an investigation by declining to take enforcement action against him.[19]

For employees facing possible criminal exposure, their incentives are even clearer: cooperation with investigators brings rewards that cooperation with compliance personnel cannot. That lesson was highlighted in 2012, as the government cooperators were sentenced in the Galleon saga that brought down Raj Rajaratnam. Of the eight cooperators sentenced in 2012, none received prison time; the worst sentence doled out was six months of home detention and the remaining seven cooperators were sentenced by five difference judges to probation.[20]

This tracks closely all cooperator sentences in the last three years. According to one study, 16 of the 20 cooperators sentenced in that time received no prison time while cooperating defendants' sentences were on average 12% of the minimum sentence recommended by the US Sentencing Guidelines.[21] Compare that to the average 73% that non-cooperating plea bargaining defendants received, and it is clear that cooperating is an easy choice for potential defendants.[22]

Additionally, given the whistleblowing bounties of the Dodd-Frank Act, employees who learn of insider trading have additional incentives to report activity to investigators, even if they do not report this information to compliance personnel. The SEC's prior insider-trading whistleblowing bounty programme was little used and capped at 10% of the amount the SEC was able to recover.[23] In the last 20 years, it has only been used six times, totalling just over $1.15m in bounties.[24] With Dodd-Frank, the incentives have increased dramatically, as whistle-blowers are entitled to 10-30% of the amount recovered.[25] What is more, the whistleblowers are not required to internally report information of potential wrongdoing before going to the SEC.[26] In the event that they do report it internally, whistleblowers must report the information to the SEC within 120 days to be eligible for a bounty.[27]

Accordingly, although whether to cooperate ideally requires a facts-and-circumstances analysis by qualified outside counsel, the fear of draconian legal consequences might cause employees to rush into the arms of law enforcement without bothering to go through established internal channels. Given these incentives for bypassing compliance personnel, compliance programmes must focus on preventing insider trading and other law violations before they occur. Additionally, such programmes ought also to create an environment in which prompt reporting is culturally and professionally encouraged, thereby avoiding Dodd-Frank prohibitions against retaliation against whistleblowers.[28] Such an environment could consist of, at minimum, a code of ethics governing employee conduct including an insider trading policy, procedures governing the effective operation of such codes, and mechanisms ensuring prompt and consistent enforcement action in response to code violations.[29]

Organisations should also seek otherwise to punish and reward behaviours in a manner appropriately supporting a values-based approach to ethics and legal compliance. Moreover, companies and other organisations, with the assistance of outside counsel, should try to identify risks and vulnerabilities to make sure adequate compliance processes are in place. Organisations with such programmes will be well positioned to benefit from SEC policies and federal sentencing guidelines that place a premium on effective corporate compliance programmes.[30] The US Department of Justice states that it will consider whether an organisation has an effective compliance programme in deciding whether to seek an indictment of the company in the event that employees engage in criminal conduct. Among a criminal prosecutor's considerations is "whether a corporation's compliance programme is merely a 'paper programme' or whether it was designed and implemented in an effective manner", including whether the programme is adequately resourced.[31]

Walking the tightrope: monitoring social media

According to April Brooks, Special Agent in charge of the New York field office of the FBI, in the coming months investigators will be mining social media, such as Twitter, for clues on insider trading.[32] Twitter can be used to distribute information and can be an early indicator of changing sentiment on stocks and commodities.[33] Firms need to be very careful, and may consider: (1) monitoring how their employees use social media; (2) having well-thought-out policies and procedures for using social media; and (3) making sure there is a strong segregation between how social media is used for social and business purposes.

A report from the Financial Industry Regulatory Authority (FINRA), the private organisation that regulates US securities brokerage firms, indicates that firms are currently relatively weak at this.[34] However, just because employers have the technical means to access the social networking information of their employees or prospective employees does not mean they have the legal right to do so. For example, employers could get in trouble



if they use Facebook "friends" to secretly gain access to their employees' otherwise private information, and they should refrain from using information obtained from social networking websites to discriminate against prospective employees. Therefore, companies should consult with counsel to ensure that any monitoring of employee media fully complies with state and federal law.

Final thoughts

Insider trading activity creates significant risk for the entities that employ or are affiliated with the individuals who engage in this prohibited conduct. In today's high-stakes enforcement environment, organisations and compliance professionals should take steps to ensure that compliance processes are in place to prevent and detect insider trading activity before the government does.

J.P. Hanlon and Michael MacPhail are Partners and Kevin Kimmerling is an Associate with the international law firm Faegre Baker Daniels LLP. They focus on white collar criminal litigation defense, internal investigations, and investigations by the Securities and Exchange Commission, Financial Industry Regulatory Authority, Department of Justice and other bodies.

1. Larry Neumeister, Feds Allege a Massive Insider Trading Scheme, Associated Press, January 19, 2012, available at 2012 WLNR 1259291.
2. http://www.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112129,00.html
3. Neumeister, supra note 1.
4. http://money.cnn.com/2012/01/24/news/economy/insider_trading/index.htm.
5. http://www.reuters.com/article/2012/11/26/investment-summit-fbi-idUSL1E8MP2IY20121126
6. Randall Fons, Joel C. Haims, Carl H. Loewenson, and Jordan Eth, Morrison & Foerster's 2012 Insider Trading Annual Review, MONDAQ, http://www.mondaq.com/unitedstates/x/217938/White+Collar+Crime+Fraud/Morrison+Foersters+2012+Insider+Trading+Annual+Review (hereinafter "Morrison & Foerster's").
7. http://www.bloomberg.com/news/2012-10-25/rajaratnam-appeal-judges-voice-concern-over-u-s-wiretaps.html.
8. http://www.reuters.com/article/2011/11/08/us-galleon-rajaratnam-idUSTRE7A76Y920111108?feedType=RSS&feedName=businessNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FbusinessNews+%28Business+News%29.
9. Cheryl Krause, Defense Strategies and Compliance Issues in the New Insider Trading Environment, Champion, Sept./Oct. 2012, at 46, 48.
10. Complaint, SEC v. Scott Allen and John Michael Bennett, Case No. 11-Civ-6443, at 61-63 (S.D.N.Y. Sept. 15, 2011).
11. Morrison & Foerster's, supra, note 6.
12. https://www.sec.gov/litigation/investreport/34-44969.htm.
13. See 15 U.S.C. § 78u-1 (authorising penalties for insider trading which "shall not exceed the profit gained or the loss avoided….").
14. http://www.sec.gov/news/press/2012/2012-16.htm.
15. Morrison & Foerster's, supra, note 6.
16. http://www.bloomberg.com/news/2012-12-06/diamondback-to-close-down-as-investors-pull-520-million.html
17. Id.
18. http://www.sec.gov/news/press/2010/2010-6.htm.
19. http://www.sec.gov/litigation/litreleases/2012/lr22298.htm
20. Morrison & Foerster's, supra, note 6.
21. Id.
22. Id.
23. http://www.sec.gov/news/press/2011/2011-116.htm (hereinafter "SEC Whistleblower").
24. Sarah L. Reid & Serena B. David, The Evolution of the SEC Whistleblower: From Sarbanes-Oxley to Dodd-Frank, 129 Banking L.J. 907 (2012).
25. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub.L. 111-203, H.R. 4173 §§ 748 and 922(a) (2010).
26. SEC Whistleblower, supra, note 26. However, the SEC maintains that "participation in an entity's internal compliance and reporting systems is a factor that can increase the amount of an award." Id.
27. Id.
28. Section 806 of the Sarbanes-Oxley Act prohibits employers who are covered by the act from discriminating against employees "because" the employee engaged in providing information concerning violations of the wire fraud, mail fraud, bank fraud or securities fraud statutes to a federal regulatory or law enforcement agency, any member or committee of Congress, or "a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct)"; or (2) filing or assisting in a proceeding related to "an alleged violation" of the wire fraud, mail fraud or securities fraud statutes.
29. For instance, Nasdaq Equity Rule 5610 requires codes of conduct to "contain an enforcement mechanism that ensures prompt and consistent enforcement of the code, protection for persons reporting questionable behaviour, clear and objective standards for compliance, and a fair process by which to determine violations."
30. See US Sentencing Guidelines Manual § 8B2.1, available at http://www.ussc.gov/Guidelines/2010_guidelines/Manual_HTML/8b2_1.htm.
31. http://www.justice.gov/dag/speeches/2006/mcnulty_memo.pdf.
32. Goldstein & Ablan, supra, note 5.
33. Id.
34. Ben Maiden, Eyes On Your Tweets, Compliance Reporter, Nov. 19, 2012, available at 2012 WLNR 28320554.