GIR Global Investigations Review

The unrelenting pace of SEC insider trading actions

02 November 2017

Marc Fagel and Elizabeth Dooley

Gibson Dunn & Crutcher partner Marc Fagel and associate Elizabeth Dooley analyse emerging trends from the recent spate of SEC insider trading enforcement actions.

As the US Securities and Exchange Commission (SEC) transitions into its new leadership, things have been relatively quiet on the enforcement front, and recent months have seen few cases of programmatic significance. Financial fraud cases involving public companies and their auditors, a high priority under the prior administration, have been virtually non-existent (aside from the steady trickle of FCPA cases). Similarly, the complex and cutting-edge cases against private investment fund managers, financial institutions, and providers of emerging electronic trading platforms touted by the SEC over the past several years have been few and far between. Instead, recent SEC enforcement actions have been dominated by retail fraud in the form of Ponzi schemes, oil & gas investment scams, and penny stock pump & dumps.

However, one area of the SEC's enforcement docket keeps chugging along like clockwork: insider trading. Typically comprising about 10% of the SEC caseload, there is no sign of any let up in new trading cases. While the high-profile actions against fund managers, expert networks, and other large industry players have run their course since the Galleon scandal earlier this decade, the SEC has had no trouble finding new targets for its investigations. Most cases are still brought against individual insiders and their tippees, but the SEC also continues to exert pressure on auditors and other professionals who misuse client information. Insider trading enforcement actions over the past year also highlight the SEC's foray into newer areas, including actions against IT professionals and hackers who misappropriate sensitive corporate data, as well as providers of political intelligence.

Classical insider trading cases

The majority of SEC insider trading cases continue to be traditional in nature – trading and tipping by corporate executives and employees. Recent examples of "classical" insider trading cases include: the CEO of a Silicon Valley fiber optics company charged with using secret brokerage accounts to trade ahead of his company's earnings releases and the announcement of its acquisition; a financial analyst at an online retailer charged with leaking

First published on the Global Investigations Review website, 2 November 2017
globalinvestigationsreview.com

earnings information to a former fraternity brother; and an inside accountant at a New Jersey pharmaceutical company charged with tipping several friends about clinical trial results and the company's impending acquisition (we note that the majority of cases referenced herein were settled without the parties admitting or denying the SEC's allegations).

Similarly, the past year has seen several incidents of individuals misappropriating confidential information from significant others and trading on the information or tipping others, such as: the husband of a semiconductor company employee charged with asking a friend to buy stock on his behalf, and tipping several family members, after learning his wife's company was being acquired in August; and a research scientist who traded in advance of two corporate acquisitions based on confidential information obtained from his wife, an associate at the law firm working on the deals, in July.

Such misappropriation cases are not limited to duplicitous husbands. In October 2017, the SEC charged a physician with trading on information shared in confidence by a friend, an executive at a Danish company planning to acquire a US supply chain services company. And in February, the SEC charged an individual for buying stock after being told in confidence by his brother, an insurance company executive, that his company was being acquired.

Emerging trends and SEC priorities

Traditional insider trading cases are far from the only insider trading cases the SEC is pursuing. Recent cases show other areas of interest for the SEC's Enforcement Division: outside professionals entrusted with sensitive information; an increasing focus on high-tech trading schemes; and the identification of abuses of political intelligence.

Outside professionals

The SEC continued to shine a bright light on trading by accountants, lawyers, bankers, and other professionals who misuse information obtained from their clients. SEC targets included: a law firm partner who was alleged to have traded ahead of nearly a dozen impending merger announcements involving his firm's clients, netting over a million dollars in profits for himself and a neighbor he tipped; an investment bank VP who established secret trading accounts to purchase stock and options after being approached by a private equity firm about arranging financing for an acquisition; a Silicon Valley-based auditor who traded in advance of a client's upcoming merger; and an accountant asked to provide tax advice in connection with a corporate merger who purchased stock in the target company and tipped a friend.

One important lesson to draw from these cases is that, when it comes to misappropriation by trusted advisors, the SEC has no minimum threshold. The SEC has never lacked for potential insider trading investigations, and often needs to take a pass on some smaller cases. But consistent with its general approach of seeking to maximise its scrutiny of corporate gatekeepers, the SEC is willing to clamp down on industry professionals regardless of the profitability of their trading. For example, in June 2017 the SEC brought a settled case against an auditor who netted less than US$7,500 trading ahead of a merger she learned about from her audit client; and in September, the SEC filed a litigated case against a California CPA who reaped just over US$8,000 in trading profits after the controller of a company to which he provided accounting services informed him that the company had received an acquisition offer.

High-tech trading (and detection)

Not surprisingly, given the general scrutiny of cybersecurity in the current environment, one emerging priority for the SEC has been trading based on nonpublic information stolen through account intrusions or other unauthorised computer usage. In December 2016, the SEC charged three China-based individuals with using malware to compromise the email networks of several US law firms and using the M&A information they obtained to rack up nearly US$3 million in illicit trading profits (this followed an earlier case, where, between 2015 and 2016, the SEC sued more than 40 individuals for an international scheme to hack into US newswire services, generating more than US$100 million in profits). Moreover, in August of this year, the SEC accused an IT employee of a large bank of using his access to the bank's computer network to steal confidential information about dozens of deals and passing the information to four friends, who in turn tipped others. The SEC alleges that the scheme generated several million dollars of unlawful gains for the various traders.

Such cases expose not just the increasingly technical means by which traders obtain nonpublic information, but the lengths to which they go to avoid being caught. Beyond the almost-routine use of accounts held in the names of friends and family to conduct trading activity, the SEC noted in one case the traders' "alleged use of shell companies, code words, and an encrypted, self-destructing messaging application to evade detection." Amusingly, in one case the SEC highlighted that the trader had Googled "how SEC detect unusual trade" the same day he traded (the research apparently didn't pay off). None of this is to say that decidedly low-tech schemes don't persevere; just a few years ago, the SEC related a tale of a law firm employee who passed tips scribbled on post-it notes and napkins which were then chewed up and eaten.

At the same time, these cases gave the SEC further opportunity to tout its own "enhanced trading surveillance and analysis capabilities." As heralded by new co-director of the SEC's Division of Enforcement Steven Peikin, such cases "reflect our continued use of sophisticated tools to detect and root out secretive and wide-reaching insider trading schemes."

Of course, such cases are tinged with a bit of irony given the SEC's September 2017 revelation that its own systems had been breached, with confidential information housed on the agency's EDGAR system potentially being utilised for insider trading. Whether the vulnerability of its own computer networks will temper the SEC's past suggestions that it could pursue action against companies which fail to take adequate steps to protect confidential information from being compromised remains to be seen.

Political intelligence

One final area which has given rise to recent enforcement activity is the disclosure of political intelligence. Following the crackdown on hedge fund trading by the SEC and the Department of Justice earlier this decade, the regulators set their sights on expert networks, suing several consulting firms with access to inside information for passing the information to their hedge fund clients. More recently, the government has expanded its focus to include consulting firms which specialise in political intelligence.

In May 2017, the SEC sued a former government employee turned political intelligence consultant for allegedly informing two analysts at a hedge fund advisory firm about federal regulatory changes he had learned about from a former colleague. According to the SEC, the analysts caused their firm to trade the stocks of four companies likely to be affected by the developments, generating nearly US$4 million in profits when the regulatory changes were publicly disclosed. The SEC also brought charges against the analysts and, more recently, settled with their firm for allegedly failing to maintain policies to prevent the misuse of inside information.

Emboldened by Salman?

The SEC's ongoing enthusiasm for insider trading cases was no doubt aided by its December 2016 victory in *Salman v US*. An 8-0 Supreme Court affirmed the SEC's ability to pursue tippees as long as there was the barest of personal benefit to the tipper, rejecting the recent Second Circuit decision in *US v Newman* holding that something of a more pecuniary nature must be exchanged for the tip. While *Newman* did not appear to significantly limit the SEC's willingness to pursue cases against tippees, the *Salman* ruling certainly bolstered the SEC's confidence in its insider trading program.

The *Salman* case stands in stark contrast to the trouncing the agency took a few months later in *Kokesh v SEC*, where a unanimous court ruled that a strict five-year statute of limitations applies to SEC claims for disgorgement (and even hinting that SEC claims for disgorgement might lack sufficient legal basis). The manner in which the SEC appoints the judges overseeing its administrative proceeds has also been called into question and may be heading to a Supreme Court showdown. Given legal pushback on some of the agency's core practices, the relatively wide berth given to the SEC in *Salman* provided some comfort that this component of the enforcement programme was on solid footing and the SEC could proceed with little fear of judicial pushback.

Conclusion

While some elements of the SEC's enforcement docket have slowed since the May 2017 appointment of SEC Chairman Jay Clayton and his selection of his new co-directors of the SEC's Enforcement Division, and the industry awaits indications of potential changes in enforcement policies and priorities, the steady flow of new insider trading cases serves as a cautionary tale for individuals with access to nonpublic information: These cases are not going away. Prosecuting insider trading is relatively apolitical, and the change in administration has little or no effect on such investigations. Technological advances have made it increasingly easy for regulators to quickly detect anomalous trading in advance of market-moving public announcements and to identify patterns indicative of broader trading schemes. And the more colourful fact patterns rise above some of the drier, more arcane cases that hit the Enforcement Division's radar screen, ensuring there will always be enforcement staff members eager to take on an insider trading investigation.

More broadly, the make-up of recent insider trading cases can be seen as a microcosm of the enforcement program writ large. The vast majority of SEC cases are straightforward, traditional cases unlikely to raise any eyebrows – the insider who tips a friend about an upcoming announcement, the spouse or family member entrusted with confidential information who turns around and uses it for personal gain. A number of cases are aimed at gatekeepers, the trust professionals whose conduct draws heightened scrutiny from the SEC – cases intended to serve as a deterrent effect on the actors the SEC expects to help safeguard the securities markets. And every now and then, there is a novel or groundbreaking case in an emerging area of interest, where the SEC confirms its willingness to push the envelope – the far-flung account intrusion scheme designed to purloin information from corporate computer networks, or the consultant marketing political intelligence or other insights from questionable sources to institutional investors.

First published on the Global Investigations Review website, 2 November 2017
globalinvestigationsreview.com