Bloomberg Law

Securities Regulation & Law Report™

INSIDER TRADING

Big Data and the Risks of Insider Trading

By Peter I. Altman, Kelly Handschumacher, and Jennifer Hustwitt

In the perennial quest for alpha, investment managers have turned increasingly to big and alternative data for market insights. The most prominent consumers of this data on Wall Street are managers of ''quant'' funds, which devour massive amounts of data and translate that data into investment decisions via complex algorithms. Over the past decade, assets managed by quant funds have doubled, and hit $500 billion in 2017. ''Rise of Robots: Inside the World's Fastest Growing Hedge Funds.'' *Bloomberg* (June 20, 2017). As of mid-2017, quant funds accounted for about 17% of total hedge fund assets. *Id*.

Peter I. Altman is a partner at Akin Gump Strauss Hauer & Feld LLP in Los Angeles. His practice focuses on representing investment management firms, private and public companies, and individuals in white collar and other government enforcement and regulatory matters, securities class action litigation, and internal investigations. Kelly Handschumacher is an associate in the firm's litigation practice in Los Angeles. Jennifer Hustwitt is a vice president in the financial institutions group at Marsh & McLennan in Los Angeles working with investment fund clients on risk transfer strategies and risk mitigation.

Meanwhile, an increasing amount of traditional investment managers are incorporating big data and quantitative strategies. This adoption ranges from a major use of big data at the firm-wide level, to having a dedicated team using big data, to having only a few portfolio managers or analysts using big data. According to Ernst and Young's 2017 Global Hedge Fund and Investor Survey, 78% of hedge funds reported in 2017 that they currently use or expect to use non-traditional data, which is up from the reported figure of roughly 50% in 2016.

The types of big and alternative data used by investment firms are myriad, and include social media data, credit card data, supply chain analysis, web traffic, search trends, digital footprint data, satellite imagery, weather data, point-of-sale data, and Internet of Things data.

While the use of big and alternative data implicates a wide range of legal issues, including privacy, contract, property, and unfair competition laws, this article focuses on key legal issues related to insider trading. The article provides a hypothetical of a hedge fund inadvertently trading on material nonpublic information (''MNPI'') in its data feed from a vendor. The article then explores how the elements of insider trading could apply to the hedge fund in the hypothetical. Finally, the article recommends best practices to prevent – or in the worst case, mitigate – liability for insider trading in connection with the use of big and alternative data.

Hypothetical

Imagine that you are the general counsel of an investment adviser that manages a macro hedge fund. For the past five years, one of your firm's analysts has been purchasing data from a startup that delivers parcels by drone (''Drone Startup''). The data includes information on the categories of parcels delivered, such as food or clothing, and the delivery origins and destinations of each category of parcel by zip code. Drone Startup is the sole delivery provider for a subscription clothing company, ClothesBox. Your firm has had a position in ClothesBox ever since it went public five years ago. Through its own research, your firm knows where all of ClothesBox's warehouses are, and can therefore use Drone Startup data to predict ClothesBox's sales.

Unbeknownst to you, Drone Startup's contract with ClothesBox includes a broad confidentiality provision that requires Drone Startup to keep information related to the services rendered to ClothesBox confidential. Drone Startup has never otherwise requested or received ClothesBox's consent to share its delivery data. Moreover, your firm's agreement with Drone Startup includes no clear representation from Drone Startup regarding its ability to sell data regarding its deliveries.

During the latest earnings report cycle – and for the first time since ClothesBox went public – it reported a decrease in sales. Your firm was able to predict this downturn ahead of time based on its research, and aggressively changed its position prior to the announcement. Your firm's change in position triggers an investigation by the U.S. Securities and Exchange Commission (SEC), which today uses advanced surveillance techniques and significant in-house big data digestion resources, including within the Division of Economic and Risk Analysis (DERA), the Analysis and Detection Center run by the Division of Enforcement's Market Abuse Unit, and the data crunching vendor Palantir Technologies, with whom the SEC recently entered into a multi-year services contract. *See* https://www.sec.gov/dera; ''SEC's advanced data analytics helps detect even the smallest illicit market activity.'' *Reuters* (June 30, 2017); ''U.S. securities regulator expands use of powerful software.'' *Reuters* (September 30, 2015).

After you learn that the SEC has opened an investigation into your firm's trading in ClothesBox, you wonder, is there any risk that your firm committed insider trading with ClothesBox? Was the information public if it was shared with any firm who purchased it? Was the information you got material if there were not any delivery statistics expressly matched to companies and your firm had to do its own research to figure out what deliveries likely corresponded with ClothesBox? Did Drone Startup knowingly breach a duty of trust or confidentiality? Should your firm have known that Drone Startup breached a duty? And what about all the other data that Drone Startup has sold to you that implicates other companies' deliveries?

Nonpublic Information

Under the federal securities laws, information becomes ''public'' either when it is disclosed '' 'to achieve a broad dissemination to the investing public generally and without favoring any special person or group,' '' or when, ''although known only by a few persons, their trading on it 'has caused the information to be fully impounded into the price of the particular stock.' '' *SEC v. Mayhew*, 121 F.3d 44, 50 (2d Cir. 1997) (quoting respectively *Dirks v. SEC*, 463 U.S. 646, 653 n. 12 and *United States v. Libera*, 989 F.2d 596, 601 (2d Cir. 1993)). Under the latter scenario, ''information may be considered public for Section 10(b) purposes even though there has been no public announcement and only a small number of people know of it.'' *Libera*, 989 F.2d at 601. This is because ''[o]nce the information is fully impounded in price, such information can no longer be misused by trading because no further profit can be made.'' *Id*.

In the hypothetical, Drone Startup's data is only available to firms that purchase it, so it has not been broadly disseminated to the investing public generally without favoring any special person or group. Nor has ClothesBox or any other company using Drone Startup published their delivery data. Arguably, however, the information could be public if the firms that obtain Drone Startup's data have fully impounded that information into the price of ClothesBox's stock, or the stock of any other company implicated in Drone Startup's data, such that no further profit can be made from that information. Proving this alternative scenario whereby the price of ClothesBox's stock reflects the information could require an advanced analytical study of factors such as stock price and trading volume, and ultimately could be too indeterminate and subjective to convince the SEC that the price was fully impounded.

Material Information

Under Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder, information is ''material'' if there is ''a substantial likelihood that a reasonable investor would view it as significantly altering the 'total mix' of information available.'' *United States v. Cusimano*, 123 F.3d 83, 88 (2d Cir. 1997) (citing *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988) and *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976)). The SEC has taken the position previously that although trading on ''material'' information from insiders is prohibited, analysts are free to obtain information from insiders for purposes of '' 'filling in the interstices in analysis.' '' *Dirks v. SEC*, 463 U.S. 646, 659 n. 17 (1983) (quoting from the SEC's brief). However, as the Supreme Court commented in *Dirks*, this rule is ''inherently imprecise,'' such that, without additional guidance, ''neither corporate insiders nor analysts can be sure when the line is crossed'' from lawful inside information that fills interstices in analyses to unlawful MNPI. *Id*.

In a recent case, the Third Circuit affirmed a jury's insider trading conviction of a Capital One employee who, in violation of the company's confidentiality policies, downloaded and analyzed information regarding purchases made with Capital One credit cards at over 200 consumer retail companies and used that information to conduct thousands of trades in those retailers' securities. *SEC v. Huang*, 684 F. App'x 167, 168-69 (3d Cir. 2017). A key argument at trial and on appeal was whether the data collected by the defendant was material. *Id*. at 169. The Third Circuit held that even though Huang could only get information on average of about

2.4% of credit card transactions of the retailers' revenues, the information allowed Huang to predict revenue more accurately than those with only publicly available data, resulting in a 12,929% three-year return on his investment. *Id*. at 170, 173. Thus, the information was material because it significantly altered the total mix of information in the eyes of a reasonable investor. *Id*. at 173.

In the hypothetical, your firm might argue that the information obtained from Drone Startup was not material, and instead merely filled ''interstices'' in your firm's analysis. Your firm might argue that the zip code and categories of parcels information never specifically mentioned any company. However, the SEC would have a strong argument that the data was material because it allowed your firm to predict ClothesBox's (and potentially other companies') revenue more accurately than those without Drone Startup's information. Even if Drone Startup only delivered 5% of ClothesBox's packages, the SEC could argue, as it did in *Huang*, that this data was enough to give your firm an advantage in predicting ClothesBox's revenue. In other words, the SEC would likely have a strong argument that the Drone Startup data was material because it significantly altered the total mix of available information through the eyes of a reasonable investor.

Breach of Duty or Deception

Assuming the SEC could prove the Drone Startup data was MNPI, it would still need to prove that it transmitted the data to your firm in violation of a duty or through deception in order to constitute insider trading.

The government relies on two theories of insider trading – the classical theory and the misappropriation theory – to prove this key element. The classical theory applies when a corporate insider or his tippee trades in securities of the tipper's corporation based on MNPI in breach of the insider's duty to the company's shareholders. *Salman v. United States*, 137 S. Ct. 420, 425 n. 2 (2016). By contrast, the misappropriation theory applies when a person misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information, such as an employer or client. *Id*. In *Huang*, the misappropriation theory of insider trading applied because Huang breached a duty of confidentiality to his employer Capital One.

Courts have held that the misappropriation theory also applies in cases where deception is used to obtain confidential information. That is, even when there is no breach of a duty of trust or confidentiality, liability may follow upon the use of deception. For example, in *SEC v. Dorozhko*, the Second Circuit held that trading on information obtained through computer hacking could be insider trading if the information was hacked by ''deceptive'' means, such as misrepresenting one's identity to gain access to confidential information. 574 F.3d 42, 51 (2d Cir. 2009). But the court noted that it would not be clear whether deceptive means were used if hackers obtained information by exploiting a weakness in an electronic code to gain unauthorized access. *Id.*

In the hypothetical, the misappropriation theory of insider trading would apply. Drone Startup was not an insider of ClothesBox (or any other company it delivered packages for), but Drone Startup had a duty to keep ClothesBox's information confidential under the terms of their contract. Drone Startup breached that duty by selling data that incorporated ClothesBox's confidential information.

Scienter

An insider trading claim also requires a showing that the defendant acted with scienter in trading on (or tipping) MNPI in breach of a duty or in deceptively obtaining information. *SEC v. Obus*, 693 F.3d 276, 286 (2d Cir. 2012); *Dorozhko*, 574 F.3d at 51. While a tipper need not have specific knowledge of the legal nature of a breach of duty, he must understand that tipping the information would violate a confidence. *Obus*, 693 F.3d at 286. Under a civil standard, the government must prove by a preponderance of the evidence that a breach of duty or deceptive act was done either recklessly or willfully, while in a criminal case, the government must prove beyond a reasonable doubt that the breach of duty was willful. *United States v. Gansman*, 657 F.3d 85, 91 n.7 (2d Cir. 2011).

In the hypothetical, there is a strong argument that Drone Startup was at least reckless, if not willful, in breaching its duty of confidentiality to ClothesBox because Drone Startup had signed a contract expressly requiring that Drone Startup keep ClothesBox's information confidential. This analysis applies to any of the other companies that Drone Startup sold delivery information on if Drone Startup used the same type of contract with a confidentiality provision and did not otherwise receive consent to sell their data.

Tipper/Tippee Liability

Given the likely duty breach, the question becomes where this leaves your firm. Where an insider or misappropriator (the ''tipper'') discloses MNPI to a non-insider (the ''tippee''), the tipper and tippee can be held liable under certain conditions. The tipper is liable if he breached a duty by tipping MNPI, had the requisite scienter when he gave the tip, and personally benefitted from the tip. *Obus*, 693 F.3d at 285. Personal benefit is defined broadly, and can include pecuniary gain, reputational benefit, and gift-giving. *United States v. Martoma*, 869 F.3d 58, 64 (2d Cir. 2017). The tippee is liable if he '' 'knows or should know' '' that the MNPI was received from one who breached a duty and the tippee trades or tips for personal benefit with the requisite scienter. *United States v. Rajaratnam*, 719 F.3d 139, 158 n. 23 (2d Cir. 2013) (citing *Obus*, 693 F.3d at 285 (quoting *Dirks*, 483 U.S. at 660)). The government need not show ''that a remote tippee knew for certain how the initial breach of fiduciary duty occurred ... but only that the tipper's conduct raised red flags that confidential information was being transmitted improperly.'' *SEC v. Conradt*, 947 F. Supp. 2d 406, 412 (S.D.N.Y. 2013); *see also United States v. Goffer*, 531 F. Appx. 8, 16 (''The Government did not need to prove that [the tippee] knew the identity or nature of the source if he knew that the information was illegally obtained.'').

In the hypothetical, Drone Startup personally benefitted from its sale of ClothesBox's information to your firm in the form of a pecuniary gain. Meanwhile, there is a question as to whether your firm knew or should have known that the information it received from Drone Startup was in breach of Drone Startup's duty to ClothesBox. The outcome will depend in part on documentation reflecting your firm's diligence of Drone Startup and an interpretation of the representations from Drone Startup regarding its right to sell its data to you. Meanwhile, whether your firm had the requisite scienter will turn on whether it intentionally or recklessly traded in ClothesBox while in knowing possession of Drone Startup's data. This same analysis applies to any other company that you may have obtained information on from Drone Startup's data.

Alternative bases for liability

Even where a firm's use of big and alternative data does not meet the elements of insider trading, it may meet elements for other causes of action. For example, under federal law, if a firm were to obtain MNPI that a vendor obtained through computer hacking instead of deception or breach of duty, it could be subject to charges of conspiracy and violating the Wire Fraud Act (18 U.S.C. § 1343) and the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

Firms should also be cognizant of state blue sky laws, such as New York's Martin Act. Under the Martin Act, the New York Attorney General (''NYAG'') has investigated firms for conduct such as providing early access to potentially market-moving information and collecting information that could give firms an unfair advantage. For example, the NYAG investigated Thomson Reuters Corporation for releasing certain potentially market-moving information to high frequency traders two seconds before it sent the information to its general subscribers. And in 2014, the NYAG and BlackRock, Inc. entered into a settlement agreement requiring BlackRock to end its Wall Street research analyst survey program, which the NYAG alleged had provided BlackRock with an unfair advantage in predicting future analyst opinions in violation of the Martin Act and other New York law.

Of course, this is not an exhaustive list, and firms should stay up to date on evolving law, including because many jurisdictions outside the United States do not require a duty breach to prove insider dealing.

Best Practices to Mitigate Risks of Insider Trading in Connection with Big Data

So now that your firm is under investigation by the SEC for insider trading, you are wondering what steps your firm should have taken to prevent, or at least have mitigated, liability for insider trading in connection with its use of big and alternative data. To prevent and mitigate such liability, a firm should:

- Implement policies and procedures regarding the types of data the firm will permit to be used, including from which vendors, and document the firm's use of data.
- Diligence its data vendors not only upon initial selection, but also on an ongoing basis, and document that diligence. This diligence includes determining who owns the data the firm is purchasing, and verifying that its vendors have the right to sell that data to the firm for the firm's intended use.
- Obtain a representation and warranty from vendors that the data provided does not contain MNPI.
- Require vendors to indemnify the firm against any claim that data from the vendor was obtained or sold in breach of the vendor's legal duties to the sources of the data.
- Verify the amount of professional liability insurance that is carried by its vendors for potential recovery for errors on the vendor's part, such as unknowingly including MNPI in a data feed, and potentially require the vendors to maintain higher professional liability limits based on scope of services.
- Consider the firm's insurance coverage for risks associated with the use of big and alternative data.
- Compare the coverage triggers and scope of regulatory investigations coverage between its professional liability and cyber liability insurance.
- Ensure that investigations are expressly covered in its policy, given that some federal appellate courts have held that insurance coverage for claims for wrongful acts does not include government investigations. *See, e.g., MusclePharm Corp. v. Liberty Ins. Underwriters, Inc.*, 2017 BL 370892 (10th Cir. Oct. 17, 2017) (policy covering claims for wrongful acts did not include SEC investigation); *Employers' Fire Ins. Co. v. ProMedica Health Sys., Inc.*, 524 F. App'x 241 (6th Cir. 2013) (policy covering claims for wrongful acts did not include Federal Trade Commission investigation). And ensure that the investigations coverage trigger is separated from the wrongful act trigger in the policy.
- Evaluate whether data collection is contemplated within the scope of investment management services in its professional liability policy.
- Ensure that there is no insider trading exclusion in its professional liability policy.
- Assess the privacy and intangible property exclusions on its professional policies.
- Assess the limit structure between its professional and cyber liability to prevent an insurance carrier from allocating to the lower cyber limit.
- Assess the insurability of any amounts deemed to be disgorgement.

Lastly, it is important to note that the laws related to insider trading are always evolving and can be unpredictable, particularly when applied to innovative uses of data in the investment space. A firm should err on the side of caution when faced with gray areas, and engage in an ongoing assessment of the benefits versus the risks of its use of various types of data.