Securities
Regulation Daily

Wolters Kluwer

July 16, 2019

# With Friends Like These: The Insider Trading Risk Presented by Family Members, Friends, and Contractors

*By Matthew Graves, Jon Haray, and Kara Thomas Beck, DLA Piper*

A spate of recent, high-profile insider trading prosecutions and SEC actions remind that the threat that individuals will trade upon material, non-public information extends well beyond a company's employees. In these enforcement actions, the company employee shared material non-public information with a third party who subsequently either traded on the information or shared the information with another third party who traded on the information. On one level, it is easy to understand why these friends and family members want to use this information when they come into possession of it: the trading profits in some of these cases are in the hundreds of thousands of dollars (if not in excess of $1 million) and an erroneous belief exists that the authorities will never learn that they used non-public information because they are not insiders.

Unfortunately for those caught up in these investigations, prosecutors and regulators do have ways of identifying non-employees who trade on non-public information. And both the Supreme Court and the Second Circuit have recently reaffirmed that non-employees can be *criminally* liable for distributing or using this information and that employees can be *criminally* liable for passing material non-public information, if they expected the recipient of the information to trade on it. Insider trading violations by company employees can, of course, cause headaches for companies in the form of shareholder derivative suits.[1] And, regardless of whether there are legal ramifications, the individuals and companies involved in these breaches of duty are impacted. The individuals involved can see their relationships with loved ones damaged, suffer reputational harm, and lose their jobs, and companies are faced with the prospect of spending time and money trying to figure out what went wrong. Companies, obviously, cannot educate the unknown universe of non-employees who may come into contact with material non-public information about the dangers of insider trading. So, a successful compliance policy should recognize the threat posed by third parties: i) ensuring that contractors and other third parties who work for the company and possess material non-public information appreciate their obligations; and ii) explaining to employees the risks of sharing such information with friends and families, providing them with cautionary tales of what could happen should they disclose.

## Recent Cases Highlight the Extent of Liability

Insider trading can occur when an insider trades on material non-public information in violation of a duty or a third party who receives the information from an insider trades on it, knowing a

[1] *See, e.g.*, Rose Krebs, "Camping World CEO Lemonis Hit With Shareholder Suit," *Law 360*, April 18, 2019, https://www.law360.com/media/articles/1151565/camping-world-ceo-lemonis-hit-with-shareholder-suit

duty was breached or after misappropriating the information.[2] When an insider shares material, non-public information with a third party and the third party trades on that information, both the tipper (insider) and the tippee (third party) can be held liable. In a criminal case, the government must prove beyond a reasonable doubt that the tipper had an expectation that the tippee would trade on the information and the tipper must have personally benefitted from the tip.[3] For a tippee, the government must prove beyond a reasonable doubt that the tippee "participate[d] in a breach of the tipper's fiduciary duty."[4] The bar for civil liability is, obviously, lower, requiring the SEC to prove these standards by only a preponderance of the evidence.

Recent cases from the Supreme Court and the Second Circuit—a Circuit in which a large number of insider cases are brought—have reaffirmed the breadth of potential liability for both the tipper and the tippees. In *Salman v. U.S.*, an investment banker passed confidential information to his brother who, in turn, passed the information to his brother-in-law, Salman. The tipper did not receive a tangible benefit from either his brother or Salman. Despite the fact that the tipper received no tangible benefit, the Supreme Court, relying on its decision in *Dirks v. SEC*, 463 U.S. 646 (1983), held that "a jury can infer a personal benefit—and thus a breach of the tipper's duty—where the tipper . . . 'makes a gift of confidential information to a trading relative or friend.'"[5] The Court reasoned that a tipper sharing confidential, non-public information with a friend or family member with the expectation or knowledge that the friend or family member would trade on the information is essentially the same as a tipper trading on the information himself and then giving the proceeds as a gift to a family member.[6] Accordingly, if the government can produce evidence that a tipper intended or expected a family member or friend to use the information to trade, that evidence could satisfy the "personal benefit" element.

Relying on *Salman*, the Second Circuit in *United States v. Martoma* held that a tipper can be held liable when he conveyed confidential information as a gift to a tippee with an expectation that the tippee would trade on it, regardless of the tipper's relationship to the tippee: the government does not have to prove the tippee was a friendor family member or that the tipper and tippee shared a "close personal relationship."[7] The Court reasoned that the relationship between the insider tipper and the trading tippee should not be determinative of whether the tipper can be liable. Rather, if the insider expects that the person receiving the information will trade on it and it resembles a gift, the insider will be held liable as a tipper.[8] After rehearing the case, the Second Circuit maintained that objective evidence of the tipper's intent should be enough to prove a personal benefit regardless of

---

[2] *See* 17 C.F.R. 240.10b5-2. The Rule then enumerates certain situations which, among others, would constitute a duty of trust or confidence. These are 1) a person who agrees to maintain information in confidence, 2) people who have a history of sharing confidence such that the recipient should know that person communicating the information expects the recipient will maintain its confidence, and 3) when a person receives information from their spouse, parent, child or sibling unless they can prove that they should not have known to keep the information confidential. *Id.*

[3] *See Salman v. U.S.*, 137 S. Ct. 420, 427-28 (2016).

[4] *Id.* at 427, *citing Dirks v. SEC*, 463 U.S. 646, 662 (1983).

[5] *Id.* at 427-428, quoting *Dirks v. SEC*, 463 U.S. 646 (1983).

[6] *Id.* at 428.

[7] 869 F.3d 58, 69 (2d Cir. 2017).

[8] *Id.*

the relationship between tipper and tippee.[9] To illustrate the point that the tipper and tippee need not have a close personal relationship in order for this gift theory to apply, *Martoma* cited a hypothetical insider, who provided inside information to a "perfect stranger," informing the stranger that he could make a lot of money trading on the information.[10] The court reasoned that the relationship between the insider and the stranger should have no import because the expectation of giving the information was that the stranger would trade on it.[11] On January 24, 2019, Martoma petitioned the U.S. Supreme Court to review and reject the standard announced by the Second Circuit.[12]

Taken together, these cases allow for an inference of tipper liability when information is gifted to anyone as long as the insider expected the person to trade on the information. As such, insiders must be careful with confidential information, and companies have a vested interest in ensuring that their employees, contractors, vendors, and attorneys are not perceived as "gifting" inside information to tippees.

## Cautionary Tales

Unfortunately, several recent high-profile prosecutions have highlighted the tragic consequences that can follow when insiders disclose material, non-public information. These cautionary tales show that even when speaking with those closest to them, insiders must exercise extreme caution when discussing the confidential aspects of their jobs. Whether disclosures are made intentionally or inadvertently, those receiving, and improperly using, the information can be exposed to criminal and civil liability, and even if charges are not brought against the insiders, their careers can be impacted by trades made by those with whom they shared the information (or the string of tippees that ensued from the initial disclosure). In order to protect themselves from the costs and reputational harm associated with insider trading investigations, companies should make sure their employees, vendors, and agents are familiar not only with the law, but also the many cautionary tales that exist. Below are just a few recent resolutions:

### *The Intoxicated Tipper*

In March 2017, a former partner at a major international firm was convicted of insider trading charges.[13] The evidence at trial showed that the former partner hosted a dinner party for friends where he drank several glasses of wine and became intoxicated. One of the friends at the dinner party also happened to be his investment adviser. During the course of the meal, the former partner made statements which suggested that one pharmaceutical company, which he represented, might merge with another pharmaceutical company in the near future.[14] The investment adviser used this information to buy stock, for both himself and the former partner, in the company that was to be

---

[9] *United States v. Martoma*, 894 F.3d 64, 75 (2d Cir. 2017)

[10] *Id.* at 75

[11] *Id.*

[12] Anne Sherry, "Martoma Seeks SCOTUS Review of 'Dirks-Defying' Insider Trading Decision," Wolters Kluwer, Jan. 30, 2019, https://lrus.wolterskluwer.com/news/securities-regulation-daily/martoma-seeks-scotus-review-of-dirks-defying-insider-trading-decision/71839/

[13] Stewart Bishop, "Ex-Hunton Patent Atty Convicted Of Insider Trading," *Law 360*, March 15, 2017, https://www.law360.com/lifesciences/articles/902137

[14] *Id.*

acquired. In total, over $400,000 in profits were generated from the trades.[15] The investment adviser pleaded guilty. The former partner vigorously denied that he intended for his friend to trade on the information, and he claimed that, because of how voluminous his trading account statements were, he did not even notice that his friend had, in fact, purchased the stock on his behalf. The jury rejected his testimony and convicted him. He was sentenced to three years' probation, a $50,000 fine, and forfeiture of the $15,000 he had received from the trades made by his friend.[16] His counsel's argument that his client had already lost millions through the loss of his job and the public revelation of his crimes potentially played a role in the former partner being able to avoid incarceration.[17] The investment adviser was sentenced to six months in prison. In January 2019, the Second Circuit upheld the attorney's conviction.[18]

### *Spousal Problems*

In June 2017, the husband of an employee of a pharmaceutical company was charged civilly with insider trading, and criminal charges followed the next month. According to the indictment, the husband traded on information regarding the outcomes of drug clinical trials provided to him by his wife, who handled risk-management and compliance issues for the company.[19] The indictment alleged that the husband earned $116,000 in profits by trading ahead of public announcements about the clinical trials.[20] Compounding matters, the husband allegedly passed some of the non-public information his wife shared with him to a friend who then also allegedly traded on the information.[21] Even though the insider specifically told her husband not to trade on the information, she resigned from her job when the inquiry into the trades began. In October 2018, a jury convicted the now ex-husband on three criminal counts of insider trading.[22] In January 2019, he was sentenced to 18 months in prison.[23]

On October 30, 2017, the husband of a former associate at a major international law firm pled guilty to insider trading charges arising from confidential client information that the associate shared with her husband.[24] Documents he signed in connection with his plea agreement reflect that the attorney's husband had multiple conversations with his wife about a pending merger involving a firm client in the mining industry.[25] Armed with this information, the husband acquired over 700

---

[15] *Id.*
[16] *Id.*
[17] William Gorta, "Ex-Hunton Atty Avoids Jail For Wine-Fueled Insider Trading," *Law 360,* September 26, 2017, https://www.law360.com/articles/967990?scroll=1
[18] Jody Godoy, "2nd Circ. Upholds Ex-Hunton Atty's Insider Trading Conviction," *Law 360,* Jan. 10, 2019, https://www.law360.com/whitecollar/articles/1117274
[19] Max Stendahl, "Husband of former Ariad exec indicted for insider trading," *Boston Business Journal,* July 20, 2017, https://www.bizjournals.com/boston/news/2017/07/20/husband-of-former-ariad-exec-indicted-for-insider.html
[20] *Id.*
[21] *Id.*
[22] Aaron Leibowitz, "Ariad Exec's Ex Gets 18 Months For Trading On Drug Info," *Law 360,* Jan. 16, 2019, https://www.law360.com/articles/1119411/ariad-exec-s-ex-gets-18-months-for-trading-on-drug-info
[23] *Id.*
[24] Pete Brush, "Husband Of Ex-Linklaters Associate Cops To Illegal Trades," *Law 360,* Oct. 30, 2017, https://www.law360.com/whitecollar/articles/979750
[25] *Id.*

options to purchase the stock of one of the entities involved in the merger and made $109,420 in profits from these options after the merger was consummated.[26] When the husband pled guilty, he emphasized that his wife lacked any knowledge of his trading activity. Nevertheless, his wife is no longer employed by her law firm, and in March 2018, he was sentenced to 15 months in prison.[27]

### *Rogue Contractor*

In December 2018, the SEC filed insider trading charges against an IT contractor and two others he allegedly tipped for trading on confidential information he stole from an investment bank while doing IT work for the bank.[28] The contractor shared the information with his wife and father, and together, the contractor and his family profited approximately $600,000 by trading on the stolen confidential information.[29] They traded in anticipation of 40 different corporate events including mergers, acquisitions, and other events. The SEC charged all three defendants with various violations of securities laws.

* * *

These are just some examples of matters charged or resolved within the last year or two, and unfortunately, we could cite many more examples of similar ill-fated trading schemes. These examples show the tendency for non-public information to flow if an insider releases it, the lure of this information to those who receive it, and the fact that insiders are often not the ones actually executing these trades. Finally, these cases highlight the toll that sharing material non-public information can take: incarceration, careers and relationships ruined, massive financial penalties, and the reputational and resource harm to the companies whose confidences were betrayed.

## What Can Companies Do?

How do companies protect themselves, their employees, their vendors, and their agents from being the next cautionary tale? Companies, obviously, cannot train an unknown universe of third parties about insider trading laws and the consequences of violating them. So, how do you stop them from acting? Simply put, you deprive them of the material non-public information. The best way to try to contain the leaks is to have a compliance program that not only warns insiders of the danger of trading on inside information, but also the dangers of merely disclosing it—particularly to loved ones. Two elements that companies should consider adding to their existing compliance program are:

- *A policy that addresses both trading and disclosure*: A company's policy should make clear that disclosure of confidential information is, in and of itself, a violation of policy that could result in termination or other adverse action. Moreover, the policy should explain why disclosure is so

---

[26] *Id.*

[27] Pete Brush, "Physicist Gets 15 Months For Trading On Linklaters Clients," *Law 360,* March 30, 2018, https://www.law360.com/articles/1028214/physicist-gets-15-months-for-trading-on-linklaters-clients

[28] SEC Halts Alleged Insider Trading Ring Spanning Three Countries, SEC Litigation Release No. 24371, Dec. 10, 2018, https://www.sec.gov/litigation/litreleases/2018/lr24371.htm

[29] *Id.*

significant, and the damage that even seemingly innocuous disclosures to loved ones can do to both the company *and* the insider. This policy should be shared with not only employees, but also the contractors, vendors, and attorneys the company retains. Such a policy puts everyone on notice of the potential risks involved with sharing the company's non-public information and helps to explain that, at the end of the day, such a policy protects them as much as it protects the company; and

- *A training program that addresses the perils of disclosure*: When not done well, compliance training can be little more than a laundry list of dos and don'ts that is about as engaging as the terms and conditions portion of an online application. While it might be a challenge to present certain issues in the compliance space in an engaging manner, the perils of disclosure are not such an issue. There is, undoubtedly, a there-but-for-the-grace-of-God-go-I quality to each of the cases described above. They are both tragic and compelling. And the insider, in a number of instances, is guilty of nothing more than indiscretion. Highlighting cases such as these—and the individuals involved in them—is likely to resonate with the listener.

## Conclusion

Both companies and insiders have a vested interest in ensuring that insiders do not disclose material non-public information: once the information explodes out of the company, there is no accounting for where it will go or how it will be used. It is important that employees, contractors, vendors, and attorneys understand the consequences of sharing confidential information. Both the case law and the cautionary tales should be woven into an effective compliance program that includes a strong policy and compelling training.