THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 57 No. 2 January 24, 2024

HOW RECENT CRYPTO PROSECUTIONS MAY CRACK THE U.S. CODE

Two recent prosecutions in the Southern District of New York have been called the first cryptocurrency insider trading cases, but neither case involved traditional securities fraud charges. Instead, both the OpenSea and Coinbase cases charged insider trading behavior as wire fraud, alleging that by trading in certain crypto assets, the defendants had misappropriated confidential business information. This theory of fraud, endorsed in Carpenter v. United States, 484 U.S. 19 (1987), let the government avoid the complexities of Title 15 insider trading law. Yet the Second Circuit has defined "confidential business information" in a variety of ways. A review of those cases and their application in the OpenSea prosecution shows how Carpenter-based theories may face legal challenges comparable to those that prosecutors sought to avoid. No matter how those challenges ultimately are resolved, prosecutors and practitioners may be in for yet another period of instability in insider trading law.

Brian A. Jacobs, Thomas A. McKay and A. Dennis Dillon *

On August 2, 2021, Nathaniel Chastain purchased a digital drawing of an anthropomorphic Tyrannosaurus shooting a laser at a skateboarding rabbit. The illustration, entitled "The Brawl 2," was tied to a digital asset known as a non-fungible token or "NFT"; NFTs use blockchain technology to prove ownership and transfer of property.[1] Hours later, Chastain sold his new asset — at twice the price. A week later, he purchased another outlandish NFT, once more selling it soon afterward at a significant multiple. And a few weeks later, he did the same thing again, making a 400 percent profit. What happened between each purchase and sale? Chastain's employer, the NFT exchange OpenSea, featured these NFTs on its home page. This event was no coincidence: Chastain was responsible for deciding which NFTs to feature and timed his sales to take advantage of the spike in value that accompanied an NFT's placement on OpenSea's home page.

[1] Indictment, *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 1 (S.D.N.Y. May 31, 2022) at 5. Chastain's appeal remains pending, and all facts concerning his conduct described in this article are as alleged.

* *BRIAN A. JACOBS and THOMAS A. MCKAY are members of Morvillo Abramowitz Grand Iason & Anello P.C. Brian previously served as an Assistant U.S. Attorney in the Criminal Division of the U.S. Attorney's Office for the Southern District of New York, where he was Deputy Chief of Appeals. Tom also previously served as an Assistant U.S. Attorney in the U.S. Attorney's Office for the Southern District of New York, where he was Co-Chief of the Public Corruption Unit. A. DENNIS DILLON is an associate at Morvillo Abramowitz. Their e-mail addresses are bjacobs@maglaw.com, tmckay@maglaw.com, and ddillon@maglaw.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

Meanwhile, on August 10, 2021, Nikhil Wahi purchased approximately $60,000 in Tribe, a new cryptocurrency.[2] A day later, he sold his Tribe tokens for a $7,000 profit. And a few months later, he did the same quick purchase and sale with a basket of new cryptocurrency tokens, making another $13,000. What happened between each purchase and sale? Coinbase — which employed Nikhil's brother Ishan — listed these cryptocurrencies on its exchanges. Again, no coincidence: Ishan tipped Nikhil off to an upcoming listing so that Nikhil could benefit from the ensuing price bump.

Despite the new subject matter, this conduct was in some ways classic insider trading: illicit use of material non-public information to engage in transactions for private gain. Federal authorities charged both men with criminal offenses within months of their trades. But neither case was charged as securities fraud under Section 10(b), the Title 15 statute that prosecutors typically use in traditional insider trading cases. Nor were the cases charged under Title 18, Section 1348, the criminal securities fraud statute. Instead, both cases were charged as simple wire fraud, in violation of Title 18, Section 1343.

By turning to their "true love"[3] in these cases, rather than Section 10(b) or Section 1348, prosecutors avoided the difficult question of whether cryptocurrencies or NFTs are "securities," because mail/wire fraud does not require the offense to be "in connection with the purchase or sale of [a] security."[4] This approach also allowed prosecutors to exchange the unstable legal ground of Title 15 insider trading law, which has seen a series of unpredictable shifts amidst fights over tippee liability,[5] for what they might have hoped was the firmer foundation of federal mail/wire fraud jurisprudence. The prosecutors' success in these crypto cases — guilty pleas from the Wahis, and Chastain's conviction at trial — perhaps will encourage future insider trading prosecutions using the same legal theory rooted in Title 18. But in stepping away from the troubled areas of traditional insider trading law in Title 15, prosecutors may have jumped from the frying pan into the fire, as these cases raise significant questions about the definition of "money or property" — a crucial limitation on the scope of mail/wire fraud charges — and when confidential business information qualifies as "property."[6]

[2] Indictment, *United States v. Wahi et al*., No. 22-cr-392 (LAP), Dkt. 1 (S.D.N.Y. July 19, 2022) at 9.

[3] Jed S. Rakoff, *The Federal Mail Fraud Statute (Part 1)*, 18 Duq. L. Rev. 771 (1980) ("To federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart — and our true love. . . . [W]e always come home to the virtues of 18 U.S.C. § 1341, with its simplicity, adaptability, and comfortable familiarity.").

[4] 15 U.S.C. § 78j(b); *see also* 18 U.S.C. § 1348 (criminalizing fraud "in connection with any commodity for future delivery, or any option on a commodity for future delivery, or any security").

[5] Brian A. Jacobs, *How Institutional Dynamics Have Shaped Insider Trading Law*, 51 Rev. Sec. & Commod. Reg. 247, 254 (Nov. 21, 2018) (describing the "problematic ambiguit[ies]" resulting from the Second Circuit's two opinions in *United States v. Martoma*). More generally, in recent years the Supreme Court repeatedly has curbed textually untethered readings of federal fraud statutes. *See, e.g., Ciminelli v. United States*, 598 U.S. 306, 317 (2023). Traditional insider trading jurisprudence, which relies primarily on the common-law development of Section 10(b) and Rule 10b-5, sits poorly with this trend.

[6] The relevant portion of 18 U.S.C. § 1343, the wire fraud statute, reads: "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for *obtaining money or property* by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both." 18 U.S.C. § 1343 (emphasis added). To fall within the statute, the scheme must target money or property. *Ciminelli v. United States*, 598 U.S. 306, 312 (2023). 18 U.S.C. § 1341, the mail fraud statute, has similar operative language and courts construe its terms — including "money or property" — alike. *Id*. n.2.

In this article, we discuss the evolution of the "confidential business information" theory of mail/wire fraud, its application to the recent cryptocurrency prosecutions, and some issues this new application raises. First, we describe the legal foundation of this theory, starting with *Carpenter v. United States* and continuing through the Second Circuit's major cases interpreting that precedent. Second, we show how the parties and the court have applied this body of law in the only cryptocurrency insider trading case to be litigated thus far, *United States v. Chastain*, and highlight some unusual aspects of the legal positions in that case. Finally, we address how prosecutions based on a *Carpenter* theory could be applied to a wider range of conduct, and some challenges the government may face in bringing such cases.

CONFIDENTIAL BUSINESS INFORMATION AS "PROPERTY": *CARPENTER* AND ITS PROGENY

The elements of mail/wire fraud are: (1) a scheme to defraud; (2) money or property as the object of the scheme; and (3) use of the mails or wires to further the scheme.[7] In *Carpenter*, in 1987, the Supreme Court held that "confidential business information" satisfied the "property" element, such that schemes involving misappropriation of such information could be prosecuted as mail/wire fraud, even though they did not target tangible property.[8] Since then, *Carpenter* has proved a crucial resource for the government.

Carpenter itself involved trading based on the *Wall Street Journal*'s "Heard on the Street" investment analysis column, which contained no inside information, but was sufficiently influential to affect prices. One of the writers of that column agreed to give two brokers advance notice of the timing and contents of the column, on which they and one of their clients traded. The writer (Winans), his partner (Carpenter), and one of the brokers were indicted in the Southern District of New York on charges that included both insider trading in violation of Section 10(b) as well as mail and wire fraud. The men were convicted at trial. Their convictions were upheld by the Second Circuit, and the Supreme Court granted certiorari to address several questions, including the petitioners' contention that the timing and contents of the newspaper column were not the *Wall Street Journal*'s "money or property," and so the related mail/wire fraud counts could not stand.

In a unanimous opinion, the Supreme Court had "little trouble" rejecting the petitioners' argument that information about the column was not money or property. The Court pointed to several specific traits that made the timing and contents of the column the *Journal*'s "property": (1) that the *Journal* had generated the information in "the course and conduct of its business," (2) that such information was gathered through the *Journal*'s own investment and was the "stock in trade" essential to its business [*i.e.*, had economic or commercial value to the *Journal*], and (3) that the *Journal* had an "exclusive" right to use that information — a fact that the Court noted was an "important aspect of confidential business information and most private property for that matter."[9] The Court further concluded that it was not necessary to prove that the *Journal* had set out written policies requiring employees to keep the contents of the column confidential, though that fact facilitated the government's proof. Having settled the question of "property," the Court found that Winans had schemed to defraud the *Journal* of that property, reasoning that by divulging the confidential business information entrusted to him he had violated a duty to his employer not to take advantage of that confidence for personal gain.[10]

Soon after *Carpenter*, the Second Circuit had another opportunity to examine a mail/wire fraud prosecution based on the misappropriation of confidential business information to trade securities. In *United States v. Grossman*, the defendant was an associate at the law firm Kramer Levin.[11] Grossman learned through a conversation with a coworker that the firm was involved in an upcoming transaction concerning Colt, the gun manufacturer. Shortly thereafter, he made dozens of calls to various friends and relatives, who then made "massive purchases" of call options on Colt stock, profiting from a spike in the share price after the transaction (a recapitalization) was announced.

[7] *Fountain v. United States*, 357 F.3d 250, 255 (2d Cir. 2004).

[8] 484 U.S. 19, 28 (1987).

[9] *Id*. at 26–27.

[10] It is notable that the petitioners also sought review of the Title 15 securities fraud counts, which relied on a misappropriation theory analogous to the wire fraud counts, because Winans was not a traditional "insider" of the companies whose securities were involved. The Court did not, however, reach the validity of the misappropriation theory in this context, affirming the decision below only because the justices were equally divided on the issue. It would be another decade before the Court endorsed the "misappropriation" theory of insider trading liability under Section 10(b) in *United States v. O'Hagan*, 521 U.S. 642 (1997).

[11] 843 F.2d 78, 79 (2d Cir. 1988).

Grossman was charged with both securities fraud in violation of Section 10(b) and mail fraud, and convicted at trial.

On appeal, Grossman argued (among other things) that his mail fraud convictions could not stand because Kramer Levin lacked a cognizable property interest in the information about the upcoming Colt transaction. In support, Grossman pointed to the traits the Supreme Court had identified in *Carpenter* and argued that none of them were present in his case: the information had no commercial value to Kramer Levin, the firm did not gather the information through its own efforts or investment, and the firm did not have exclusive rights to exploit the information.

The Second Circuit declared this claim "specious." The court found that Grossman "distort[ed] *Carpenter*," and that these traits — commercial value, acquisition in the course of business through its efforts, and exclusivity — "*describe[d]*" rather than defined the property at issue in *Carpenter*. From that characterization of *Carpenter*, the Circuit proceeded very quickly to its conclusion, stating:

> *Carpenter* actually holds *generally* that, even though "confidential business information" is intangible, it "has long been recognized as property." Thus, the information in this case regarding the Colt recapitalization clearly falls within the definition of property under *Carpenter*.[12]

In other words, rather than engaging in substantive discussion of what might have made Kramer Levin's information about the upcoming transaction "property," the Circuit simply assumed the information Grossman used was "confidential business information," and thus property. Perhaps sensing a weakness in this quick conclusion, the Circuit then added that the information *did* have commercial value to Kramer Levin, because maintaining a reputation for maintaining confidentiality could protect the firm's business prospects. Grossman sought Supreme Court review but was denied.

Perhaps because *Grossman*'s holding discouraged subsequent litigants from asserting their schemes did not target "property," it was more than 20 years before the Second Circuit returned in detail in *United States v. Mahaffy*[13] to the issue of "confidential business information." *Mahaffy* concerned a front-running scheme that relied on information obtained from brokerages' "squawk boxes." Squawk boxes were office-wide intercom systems, through which brokers discussed news, exchanged information, and occasionally announced customer orders so that other brokers could see if they had counterparties who might take the trade. A day-trading firm enlisted employees of multiple Wall Street brokerages to place a telephone call to the day traders, leave their telephone receivers near their squawk boxes, and thereby give those day traders a live feed of any block trades announced over the squawk boxes. Using that advance notice, the day traders could front-run the trades and profit.

The defendants were charged (among other things) with securities fraud under Title 18, Section 1348, and conspiracy to commit securities fraud. Although the fraud charges were brought under Section 1348 rather than as mail/wire fraud, the theory of the fraud was still based on *Carpenter*: the government alleged that the defendants had conspired to misappropriate the brokerages' property, *i.e.*, the confidential business information regarding customer orders conveyed over the squawk boxes. After two trials, the defendants were convicted of that conspiracy.

A "critical issue" at trial and on appeal was whether the information shared over squawk boxes actually was confidential. The parties did not dispute that the squawk boxes typically conveyed mere chatter, not confidential information belonging to the brokerages; the issue was whether the specific discussion of customer trades was confidential. Evidence on that point was mixed. Several executives testified that they expected their employees to maintain confidentiality surrounding clients' block trades, claiming confidentiality regarding customer orders was a "basic concept" and that such information should only be "used on a need-to-know basis." The relevant corporate policies also generally required caution in disclosing client orders. But there also had been testimony that none of the brokerages had policies specific to maintaining confidentiality of "squawked information," and that the brokerages did not take comprehensive steps to limit who — including visitors — could hear the squawked information on the firms' premises. There also was evidence that brokers "were expected to share clients' block orders with certain other clients," even if they were supposed to do so judiciously.

The Second Circuit found this record sufficient to show the use of squawked information about customer trades constituted misappropriation of confidential business information under *Carpenter*. The Circuit said that under *Carpenter*, "a business's information may be confidential if [(1)] the business exclusively possesses

[12] *Id.* at 86 (emphasis added) (citation omitted).

[13] 693 F.3d 113 (2d Cir. 2012).

the information and [(2)] considers it to be, and treats it as, confidential."[14] The Circuit found adequate to establish these two factors the executive testimony that the brokerages generally expected their employees to keep customer trades confidential, as well as testimony that even if squawks could be heard by visitors or employees without a need to know, the firms did not allow others to "listen directly to squawks or hear squawks in their entirety," thus preserving their exclusive possession of the information.

Despite this conclusion, the Circuit vacated the convictions because it found the prosecutors had suppressed exculpatory evidence by deciding not to turn over transcripts of SEC testimony in which witnesses said that "squawked information was not confidential and that no firm policies prohibited the direct transmittal of squawks outside each respective firm."[15] In the new trial, the Circuit said, the district court's "instruction regarding confidential business information should provide more fulsome guidance to assist the jury in determining whether the squawked information was confidential." By way of elaboration, the Circuit reiterated that "*Carpenter* requires proof that the information was both considered and treated by an employer in a way that maintained the employer's exclusive right to the information."[16] The "pertinent factors" to this determination, the Circuit said, included "written company policies, employee training, measures the employer has taken to guard the information's secrecy, the extent to which the information is known outside the employer's place of business, and the ways in which other employees may access and use the information." The Circuit ended this guidance with a word of caution: "If employers 'consider' information to be confidential but do not really take affirmative steps to treat it as such and maintain exclusivity, *Carpenter* is not satisfied."[17]

Mahaffy offered valuable clarification of when business information would be considered confidential. But *Mahaffy* seemed to suggest — in tension with *Grossman* — that exclusivity was a necessary characteristic (and, with confidentiality, a sufficient characteristic) of confidential business information.

[14] *Id*. at 121 n. 7.

[15] *Id*. at 127–28.

[16] *Id*. at 135 n. 14.

[17] On remand, all defendants negotiated deferred prosecution agreements with the government, meaning the Circuit's instructions were not tested in practice.

UNITED STATES V. BLASZCZAK: SHIFTING OPINIONS ON WHAT MAKES INFORMATION "PROPERTY"

Seven years later, *Blaszczak* returned to the same question in a case concerning trading based on confidential information obtained from the Centers for Medicare and Medicaid Services ("CMS").[18] Blaszczak, a former CMS employee, provided investors at two hedge funds certain "pre-decisional information," mostly about upcoming reimbursement rate changes, that he obtained from friendly employees still working at the CMS. The investors then used Blaszczak's information to trade stocks that would be affected by the reimbursement rate changes before these changes were announced. Southern District of New York prosecutors charged the defendants with (among other things) violations of Section 10(b), Section 1348, and wire fraud. The defendants who went to trial were acquitted of all Title 15 counts but were convicted on most of the Title 18 charges.

On appeal, the defendants raised several issues — including whether the Title 18 securities fraud and wire fraud statutes required proof of a "personal benefit" like Section 10(b) did — but also argued that the "pre-decisional information" at issue was not "property," because it was not confidential business information within the meaning of *Carpenter*. The defendants argued that their conduct at worst constituted interference with the government's exercise of its regulatory authority, instead of its rights as a property holder. The defendants' interpretation would have meant the prosecution was foreclosed by *Cleveland v. United States*, 531 U.S. 12 (2000), in which the Supreme Court found an alleged scheme to obtain licenses to operate video poker machines did not target the government's "money or property," but rather a mere regulatory interest, and so could not be prosecuted as mail/wire fraud.

The Second Circuit, in an opinion by Judge Sullivan, joined by Judge Droney (who retired shortly after the opinion's issuance), and over a dissent by Judge Kearse, rejected the defendants' interpretation and held that the CMS pre-decisional information was property under *Carpenter*.[19] While the opinion focused on distinguishing *Cleveland*, it also independently discussed how courts might conclude information was property, namely by identifying a "right to exclude that is

[18] *United States v. Blaszczak*, 947 F.3d 19, 26 (2d Cir. 2019) ("*Blaszczak I*").

[19] *Id.* at 33.

comparable to the proprietary right recognized in *Carpenter*." The court thus reiterated *Mahaffy*'s view: that confidentiality and exclusivity were the defining characteristics that made information an entity's property.[20]

Not long after the Second Circuit issued this opinion, however, the Supreme Court decided *Kelly v. United States*, the so-called Bridgegate case.[21] In *Kelly*, the Court held that schemes involving the government's rights of "allocation, exclusion, and control," and only incidentally affecting the government's money or property, could not be charged under the Title 18 fraud statutes. The defendants in *Blaszczak* made this decision a centerpiece of their petition for certiorari, and the Supreme Court vacated the Second Circuit's opinion and remanded the case for further consideration on the question of "property."[22] On remand, the government confessed error, stating the Department of Justice's new position that "information typically must have economic value in the hands of the relevant government entity to constitute 'property.'"[23] The Second Circuit, in an opinion by Judge Kearse (who had dissented in *Blaszczak I*) which Judge Walker joined, agreed with the government that vacatur was necessary, finding that "[w]hile confidential information may constitute property of a commercial entity such as the publisher victim in *Carpenter* . . . the same is not true with respect to a regulatory agency such as CMS."[24] The distinction, in the Circuit's view, was economic value: while the *Wall Street Journal* was a business "for which confidential information was its stock in trade . . . to be distributed and sold to those who would pay money for it," CMS was "not a commercial entity; it does not sell, or offer for sale, a service or a product." In other words, premature disclosure of a regulatory decision had "no direct impact on the government's fisc," and even if disclosed, the decision "remain[ed] within the exclusive control of CMS."

In dissent, Judge Sullivan — who wrote the original opinion for the majority in *Blaszczak I* — maintained that the CMS pre-decisional information was "property" notwithstanding *Kelly*.[25] Judge Sullivan pointed in particular to *Carpenter*'s discussion of the right to "exclusive use" as a core aspect of a property right in confidential information, and CMS's similar right to exclusive use of the pre-decisional information. Because the scheme was intended to use that information for private gain, rather than influence a governmental decision or alter a regulatory choice, Judge Sullivan argued the case required nothing more than a straightforward application of *Carpenter*. Judge Sullivan also pointed out that requiring property to be a company's "stock in trade" countermanded other decisions based on misappropriation of confidential information that had nothing to do with a company's ordinary business.[26] The majority in *Blaszczak II*, however, arguably shifted the analysis away from the right to exclude that was central to *Carpenter*, *Mahaffy*, and *Blaszczak I*, and put the focus on economic or commercial value.

UNITED STATES V. CHASTAIN: THE GOVERNMENT AND THE COURT APPLY *CARPENTER* TO A NEW SET OF FACTS

In between the two *Blaszczak* opinions, the government brought the two cryptocurrency insider trading cases that introduced this article. The *Wahi* case, involving advance notice of Coinbase listings, was resolved relatively quickly with guilty pleas from the two Wahi brothers, meaning the government's theory of fraud was not tested.[27] Chastain, however, went to trial

[20] The court further stated (in a passage that paralleled *Grossman*) that even if economic value was not a necessary characteristic of "property," CMS did have an economic interest in the pre-decisional information because it had invested resources in "generating and maintaining the confidentiality" of that information, and those resources would be "devalued" if the information were leaked.

[21] 140 S. Ct. 1565 (2020). The defendants in *Kelly* had sought to punish the mayor of Fort Lee for his refusal to endorse Governor Chris Christie by closing lanes that Fort Lee commuters used to access the George Washington Bridge.

[22] *United States v. Blaszczak*, 141 S. Ct. 1040 (Mem.) (2021).

[23] *United States v. Blaszczak*, 56 F.4th 230, 236 (2d Cir. 2022) ("*Blaszczak II*").

[24] *Id*. at 243.

[25] *Id*. at 250.

[26] *Id.* at 256. Judge Sullivan cited *O'Hagan*, which concerned a scheme to take advantage of information regarding a tender offer, rather than information that was the stock in trade of the company at issue, as well as *United States v. Khalupsky*, 5 F.4th 279, 285 (2d Cir. 2021), which held that hacking of pre-publication press releases constituted a scheme to defraud and use of a "deceptive device" within Section 10(b), and *SEC v. Dorozhko*, 574 F.3d 42, 44 (2d Cir. 2009), which held that the SEC was not required to allege or prove a breach of fiduciary duty to allege a violation of Section 10(b) where the conduct had involved the hacking of MNPI.

[27] A third defendant in *Wahi* lives abroad and has not yet been arrested.

after extensive pre-trial litigation over the application of *Carpenter*, and his case remains pending on appeal. These cases were not only the first cryptocurrency insider trading cases but also among the first prosecutions in the Second Circuit to apply *Carpenter*'s mail/wire fraud doctrine outside of the securities context. The *Chastain* case, in particular, illustrates some of the complexities of applying the Second Circuit's case law, and the impact that differing definitions of "confidential business information" may have on liability.

As described above, Nathaniel Chastain worked at OpenSea, a large online marketplace for trading NFTs.[28] He was responsible for selecting the NFTs that would be featured on OpenSea's home page. Once featured, the price of those NFTs typically would increase substantially. The indictment alleged that on approximately 11 occasions, Chastain misappropriated the information about which NFTs would be featured to buy those NFTs before they were featured, benefiting from the subsequent price pop. The indictment further alleged that Chastain had an obligation to keep this information — along with "any information not generally known or available outside of OpenSea" — confidential and that he had signed a confidentiality agreement to that effect. By using that information to trade for his own benefit, the indictment alleged he had committed wire fraud.

Chastain moved to dismiss the indictment. He contended (among other things) that information about which NFTs would be featured was not "confidential business information" under *Carpenter*, and hence not OpenSea's "money or property."[29] He argued that his thoughts about which NFTs to feature were not property because they had no "inherent economic value" to OpenSea. In the same vein, he argued that *Carpenter*, especially given its discussion of how confidential information was the *Journal*'s property in part because it was the newspaper's "stock in trade," was restricted to information of the type the company was in the business of selling. The government responded that *Grossman* had "rejected" the idea that only information that was commercially exploitable was property under *Carpenter* and that *Mahaffy* left "no doubt that 'property' is not limited to 'stock in trade' that an employer sells," because Kramer Levin did not trade in the information at issue in that case.[30]

The court declined to resolve the dispute at the motion to dismiss stage, but the issue arose again when the parties proffered expert testimony bearing on the same question. In the related briefing, the government stated its view:

> The information just needs to be 'confidential business information,' which is information a company creates or acquires for a business purpose (the 'business' part) that the company considers and treats as confidential (the 'confidential' part).[31]

The court agreed, determining that the government need not prove the information had "inherent economic value" to establish a scheme targeting money or property.[32]

The court began its analysis with *Carpenter*, interpreting that decision to say "it was enough for the Government to prove (1) that the information at issue was kept confidential by the *Journal* and (2) that it was 'acquired or compiled . . . in the course and conduct of its business,'" rather than having to prove the information had commercial value. The court then walked through the Second Circuit's opinions in *Grossman* and *Mahaffy*, noting that neither focused on the potential for confidential business information to have commercial value. Finally, the court turned to *Blaszczak II*, which had been issued only a few months beforehand, after Chastain had been charged and had filed his motion to dismiss. The court reasoned that *Blaszczak II* did not involve "confidential *business* information," and had invoked the "stock in trade" language of *Carpenter* "merely" to explain why the CMS information was "regulatory in character." The court concluded that even if the commercial value was *relevant* to the jury's determination whether the information at issue was OpenSea's property, it was not a necessary part of the government's proof.

The court's opinion — endorsing the government's preferred test and cabining *Blaszczak II* — is in some

[28] Indictment, *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 1 (May 31, 2022) at 1.

[29] Mot. to Dismiss, *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 17 (August 19, 2022) at 11.

[30] Opp. To Def.'s Mot. to Dismiss, *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 23 (Sept. 7, 2022) at 13, 17.

[31] Opp. To Def.'s Mot. to Exclude, *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 62 (April 5, 2023) at 7.

[32] *United States v. Chastain*, No. 22-cr-305 (JMF), 2023 WL 2966643, at *1 (S.D.N.Y. Apr. 17, 2023).

tension with the cases it interpreted. *Carpenter* indicated and *Mahaffy* confirmed that exclusive rights were necessary for confidential business information to be property. But where *Mahaffy* said that the government must prove the information was confidential, treated as such, and "that the [company] had exclusive use of [it],"[33] Judge Furman in *Chastain* said that the information must be considered confidential, protected as such, and merely "acquired or compiled . . . in the course and conduct of [the company's] business."[34] Meanwhile, *Blaszczak II*'s treatment of property rested on the lack of commercial value to CMS in the pre-decisional information.[35] But the court's opinion in *Chastain* focused on neither exclusivity nor commercial value. Instead, consistent with the government's position, the court asked whether the information was acquired or compiled in the course of the company's operation, and later instructed the jury to that effect.

Given this pre-trial ruling, Chastain's trial defense focused on the question of confidentiality, rather than whether the information was acquired or compiled in the course of OpenSea's business, or whether it had commercial value. He argued that nobody at OpenSea had told him the featured NFT information was confidential, and that the company had taken no affirmative steps to treat that particular information as confidential.[36] The government's proof as to confidentiality was limited. The NDA that Chastain had signed contained only a general obligation to hold in confidence "information . . . not generally known or available outside the company."[37] Evidence that OpenSea treated the featured NFT decision *in particular* as confidential was thin: in closing, the government pointed only to the facts that employees signed general NDAs, that corporate leadership gave responsibility for picking the featured NFTs to Chastain, a senior person in the small company, that the company didn't have a practice of telling others (including insiders) about the NFTs to be featured, and that the company took action against Chastain when his trading was discovered.[38] The jury voted to convict.

In a case like *Chastain* — or perhaps even most private-sector misappropriation cases — it may be unlikely that confidentiality would be present without exclusivity, meaning an explicit requirement that the government prove OpenSea had an exclusive right to exploit the misappropriated information, in addition to maintaining the information's confidentiality, would make little difference. Judge Furman's instructions to the jury combined "exclusivity" and confidentiality in a single sentence: he told the jury that "[i]f an employer 'considers' information to be confidential but does not take affirmative steps to treat it as such and *maintain exclusivity*, it does not qualify as property."[39] Chastain likewise did not focus on exclusivity in his pre-trial briefing. But it is equally possible to imagine — as below — a scenario in which the presence or absence of a more developed exclusivity argument might carry more weight.

It is also possible that in many private-sector cases, there will be little daylight between the court's holding in *Chastain* and the holding in *Blaszczak II*, as private businesses are not likely to assemble information without commercial value. But as described above, Chastain did emphasize before trial the theory that confidential business information must have commercial value, and the court's decision not to endorse that theory may have had more of an impact. To be sure, Chastain may still have been found guilty at trial even if the government had been required to prove that his thoughts about the featuring of NFTs had "commercial value." After all, in theory, OpenSea could have monetized those thoughts by selling advance notice that specific NFTs would be featured to a smaller group of users, for example. But OpenSea did nothing of the kind, and the selection of NFTs for featuring was hardly OpenSea's stock in trade or consistent with its business model as an exchange. Those facts may well have swayed a differently instructed jury. Chastain's appeal is pending, and may well involve argument both over the court's definition of confidential business information and whether, even under the court's ample definition, there was sufficient evidence to convict.

CHASTAIN'S BROAD IMPLICATIONS — AND POTENTIAL PITFALLS

Unless overturned on appeal, the government's victory in *Chastain* — both in the guilty verdict and the court's broad definition of confidential business information — and the quick pleas in *Wahi* may well encourage future prosecutions of similar conduct on the

[33] *Mahaffy*, 693 F.3d at 127.

[34] *United States v. Chastain*, No. 22-cr-305 (JMF), 2023 WL 2966643, at *3 (S.D.N.Y. Apr. 17, 2023).

[35] *Blaszczak II*, 56 F.4th at 236.

[36] Trial Tr., *United States v. Chastain*, No. 22-cr-305 (JMF), Dkt. 139 (May 1, 2023) at 837.

[37] *Id*. at 788.

[38] *Id*. at 794.

[39] *Id.* at 918–19 (emphasis added).

same *Carpenter* theory. Some of these prosecutions may be traditional insider trading-like cases, but not involving securities laws, as prosecutors continue to try to avoid the doctrinal confusion surrounding prosecutions under specific securities fraud statutes. Others may be in securities-adjacent spaces like the cryptocurrency cases. Yet others might be in entirely new industries.[40] In any such cases, however, prosecutors may find that they have traded the doctrinal confusion surrounding Title 15 for a new kind of doctrinal confusion surrounding the definition of "confidential business information."

One potential area for *Carpenter*-based expansion of insider trading law is real estate. Consider a scenario in which an employee of a real estate developer buys property next to a tract that he knows his employer has confidentially contracted to develop. Regardless of whether a court adopts the broad definition of confidential business information used in *Chastain* or requires some additional trait as in *Mahaffy* or *Blaszczak*, this seems to be a misappropriation of the employer's confidential business information. The employee has used information "acquired or compiled . . . in the course and conduct of [the company's] business" to identify the property and its investment potential.[41] Information about pending real estate transactions equally surely has "commercial value" to a real estate developer. And it seems likely that the developer has exclusive rights to use the information that led it to determine the development deal was a sound investment. Prosecutors well could view this case as a more straightforward application of *Carpenter* than *Chastain*.

In other areas, the expansion of *Carpenter*-based insider trading prosecutions could depend on whether the broad view of "confidential business information" adopted in *Chastain* applies. Consider, for example, the burgeoning sports betting market. Suppose a locker room attendant for the Los Angeles Lakers sees LeBron James privately requesting treatment for an ankle injury before a critical playoff game. The attendant, who knows others have yet to learn of the potential injury, places a $10,000 bet that the Lakers will lose the game. Is this "insider gambling," chargeable as mail/wire fraud under *Carpenter*?[42]

The answer may depend on how "confidential business information" is defined. If a court applies the definition used in *Chastain*, the attendant is probably liable. He has used information acquired or compiled in the course and conduct of the Lakers' business. The Lakers likely already take steps to ensure that this kind of information is kept on a need-to-know basis until disclosed, satisfying the "confidential" aspect. But does this information have commercial value to the Lakers, such that it would be "property" under *Blaszczak II*? Information about injuries is not really part of the Lakers' "stock in trade," and league policies prohibit players and employees from betting on the team at all,[43] so probably not. If the information does not have commercial value, do the Lakers at least have exclusive rights to use it? Again, probably not: among other things, absent a contract to the contrary, there is nothing preventing James from disclosing a potential injury to the public.[44]

---

[40] The Courts of Appeals have in at least a few cases already endorsed use of *Carpenter*-based theories to police a wider variety of business misconduct. In *United States v. Hager*, 879 F.3d 550, 555 (5th Cir. 2018), for example, the Fifth Circuit upheld mail and wire fraud convictions where the defendant's substantive misconduct was essentially self-dealing. The defendant, a salesperson for a computer parts distributor, used his employer's order and pricing information to identify parts that his employer would need to fulfill customer orders. Through a shell company in his wife's name, he then sold those parts to his employer at a price that he knew from his access to his employer's pricing model the employer would accept. The Court of Appeals found this evidence sufficient to convict under a *Carpenter* theory. Similarly, in *United States v. Hedaithy*, 392 F.3d 580, 595 (3d Cir. 2004), the Third Circuit found that a scheme involving sham test-takers constituted misappropriation of the confidential test questions, thereby depriving the company of its right to exclusive use of those questions and targeting the testing company's confidential business information under *Carpenter*.

[41] *Chastain*, 2023 WL 2966643, at *3.

[42] Matt Levine, *Tether Keeps Lending Tethers*, Bloomberg Opinion (Sept. 21, 2023), https://www.bloomberg.com/opinion/articles/2023-09-21/tether-keeps-lending-tethers.

[43] NBA Const. art. 35A ("No person may . . . directly or indirectly wager money or anything of value on the outcome of any game played by a Team in the league operated by the [NBA].").

[44] It is worth noting in this context that mail/wire fraud also requires deceptive conduct — typically, but not always, a misrepresentation or an omission in the context of a duty to speak — to satisfy the element of a "scheme to defraud." In *Carpenter*, the deceptive element was found in the fact that "Winans continued in the employ of the *Journal*, appropriating its confidential business information for his own use, all the while pretending to perform his duty of safeguarding it." *Carpenter*, 484 U.S. at 28. As in *Carpenter*, the other cases discussed in this article mostly did not address the deception requirement in depth, perhaps because the schemes all involved

The same definitional issues may arise even in a more traditional prosecution connected to securities trading. Consider the case of a young research analyst who, through her work, gains exposure to and experience with her employer's financial modeling techniques. She then uses that experience to develop her own models for trading on her own account, without relying on any inside information. Has she misappropriated confidential business information? The answer could depend on how specific the techniques she uses are. If they are just generally applicable modeling techniques taught in any Excel boot camp, then no. If they are sufficiently specific to constitute a trade secret, then perhaps yes. In between, she is in a gray area. The information about how to build reliable financial models surely was acquired or compiled in the course of her employer's business. That information likely has some commercial value to the employer. The employer probably also limits access to its models to protect their confidentiality. But in this in-between scenario, she potentially does *not* use any information to which her employer has exclusive rights. Is she guilty of mail/wire fraud? Under *Grossman* or *Chastain*, perhaps yes. Under *Mahaffy*, perhaps not.

Now imagine a similar case in which the same investment analyst gains deep subject-matter expertise in a particular industry, but entirely based on her analysis of public information. She then leaves her employer and sets up her own investment fund, which focuses on the same industry. Has she misappropriated her employer's confidential business information? Again, that information has commercial value, and she acquired or compiled it in the course of the employer's business. But here both confidentiality and exclusivity would be in question. The point is that the legal definition of "confidential business information" could have a real-world impact on guilt and innocence.

There are also complexities in applying *Carpenter* even to other routine fact patterns in insider trading jurisprudence. Where a tippee receives confidential business information from a family member or friend, a direct charge that the tippee misappropriated confidential business information seems less likely than a charge predicated on conspiracy or accomplice liability. In any case (whether insider trading or otherwise) those charges come with additional requirements for proof, complicating the government's task. In a tipper-tippee scenario, such charges also invite difficult questions as to knowledge and intent. For example, would prosecutors have to prove the tippee understood the information was confidential business information? Would they have to prove that the tipper received a personal benefit for his tip? *Carpenter* and its progeny do not offer a clear answer.[45]

Finally, any substantive challenge to future *Carpenter*-based cases would find support in the Supreme Court's most recent interpretation of the mail/wire fraud statute. In *Ciminelli v. United States*, the Supreme Court struck down the Second Circuit's "right-to-control" theory of wire fraud, finding that "potentially valuable economic information" was not a "traditionally recognized property interest" protected by the mail and wire fraud statutes.[46] To hold otherwise, the Court said, would be to endorse a theory "unmoored from the federal fraud statutes' text." That opinion did not reach confidential business information. (In fact, the Court cited *Carpenter* for the proposition that only long-recognized forms of property were protected.) But the note of caution *Ciminelli* strikes on broad readings of these statutes when they come to "intangible" property rights could give any court so inclined a hook for a narrow reading of *Carpenter*. The *Ciminelli* opinion was issued too late to be addressed by the district court in *Chastain* but could figure in the appellate briefing.

footnote continued from previous page…

employees misusing employers' information. In *Mahaffy*, the defendants did raise a challenge along these lines, but the court found that the defendants had violated a duty to their employer because "[e]ach brokerage firm had a policy that required employees to report violations of the firm's code of conduct," which they had broken. *Mahaffy*, 693 F.3d at 126. Prosecution of a non-employee on a *Carpenter* theory may invite additional litigation — of the kind that has been common in cases brought under Section 10(b) — regarding the existence of a duty that was breached.

[45] With respect to both Title 18 securities fraud and wire fraud, *Blaszczak I* held that no proof of a personal benefit to the tipper was required, even if such proof was required for Title 15 securities fraud; this holding was criticized in *Blaszczak II* but not reversed, leaving the "personal benefit" test in limbo. *Compare Blaszczak I*, 947 F.3d at 36 *with Blaszczak II*, 56 F.4th at 246 (Walker, J., concurring). *Carpenter* itself involved a tipper/tippee pattern, but the opinion did not address the related issues. In *Grossman*, none of the tippees apparently were charged. In *Mahaffy*, the only count of conviction was the conspiracy charge. These ambiguities may have informed the government's charges in *Wahi*. The tippees in that case were charged both as conspirators and as participants in the substantive fraud, yet as to the latter charge, the government included a citation to the general accomplice liability statute.

[46] *Ciminelli*, 598 U.S. at 314.

CONCLUSION

Even after some 40 years, the contours of criminal liability for misappropriation of confidential business information are not sharply defined. The broad view of *Carpenter* and its progeny that the government pressed in *Chastain* could open new areas of conduct to prosecution under the mail and wire fraud statutes — already prized by prosecutors for their breadth and adaptability. Whether the lower courts will limit this expansion by taking a more constrained view of "confidential business information" may determine prosecutors' initial success in such efforts. Even if prosecutors are as successful at the outset as they were in *Chastain*, whether appellate review will uphold any such cases remains an open question. Regardless of the ultimate outcome, prosecutors and practitioners may be in for yet another period of instability in insider trading law. ■

The Review of Securities & Commodities Regulation