No. 08-0201-CV

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff-Appellant

v.

OLEKSANDR DOROZHKO,
Defendant-Appellee.

On Appeal from the United States District Court
for the Southern District of New York

OPENING BRIEF OF THE
SECURITIES AND EXCHANGE COMMISSION,
APPELLANT

BRIAN G. CARTWRIGHT
General Counsel

ANDREW N. VOLLMER
Deputy General Counsel

JACOB H. STILLMAN
Solicitor

MARK PENNINGTON
Assistant General Counsel

DAVID LISITZA
Attorney

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-8010
(202) 551-5015 (Lisitza)

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (CONTINUED)

Page

TABLE OF CONTENTS (CONTINUED)

Page

TABLE OF CONTENTS (CONTINUED)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES (CONTINUED)

Page

TABLE OF AUTHORITIES (CONTINUED)

Page

TABLE OF AUTHORITIES (CONTINUED)

Page

STATUTES AND RULES

TABLE OF AUTHORITIES (CONTINUED)

Page

MISCELLANEOUS

JURISDICTION

The district court had jurisdiction pursuant to Section 27 of the Securities Exchange Act of 1934, 15 U.S.C. 78aa, over this civil law enforcement action brought by the Securities and Exchange Commission. The Commission appeals from the district court's order denying its motion for a preliminary injunction and lifting an asset freeze that the court had entered at the beginning of the litigation against defendant Oleksandr Dorozhko. JA998-1051.[1] This Court has jurisdiction pursuant to 28 U.S.C. 1292(a)(1). The district court entered its order on January 8, 2008. The Commission's notice of appeal was timely filed on January 11, 2008. Fed. R. App. P. 4(a)(1)(A).

ISSUES PRESENTED FOR REVIEW

1. Whether defendant employed a "deceptive device or contrivance" within the meaning of the antifraud provisions in Section 10(b) of the Exchange Act when he hacked into a secure computer system in order to obtain material nonpublic information about corporate earnings that he immediately used to trade in securities.

---

[1] "JA" refers to the Joint Appendix filed with this brief.

2. Whether the only conduct that can be "deceptive" under Section 10(b) is conduct that breaches a fiduciary duty.

STATEMENT OF THE CASE

A. Nature of the case

The Commission alleges that defendant Oleksandr Dorozhko committed securities fraud in violation of Section 10(b) of the Exchange Act, 15 U.S.C. 78j(b), and Rule 10b-5 thereunder, 17 C.F.R. 240.10b-5, when he hacked into a secure computer system to obtain material non-public corporate information and immediately exploited that information to buy securities. JA9-10, JA12-16. The Commission sought a preliminary injunction and asset freeze pending the outcome of the litigation, and a permanent injunction and other appropriate relief following final adjudication of its claim. JA16-17, JA27-46.

The United States District Court for the Southern District of New York (Judge Buchwald) issued a temporary restraining order and froze the proceeds of the fraudulent transactions at the time the Commission's complaint was filed. JA18-26. After conducting a hearing on the Commission's request for a preliminary injunction, the district court ruled

that the Commission was unlikely to prevail on the merits of its claim reasoning that "a breach of fiduciary duty of disclosure is a required element of *any* 'deceptive' device under § 10(b)" (JA1017-1018) (emphasis added), even in cases where the defendant affirmatively made deceptive statements or engaged in deceptive conduct, and the Commission had not presented evidence that Dorozhko had violated any such duty. JA1002. The court therefore denied the Commission's motion for preliminary injunction and ordered the freeze to be lifted, but allowed the Commission to seek a stay pending appeal in this Court. JA1049-1050. After the Commission sought emergency relief here, this Court ordered that the freeze be maintained pending its review of the district court's decision. JA1171.

B. Facts

The following statement of facts is based on the evidence introduced at the preliminary injunction hearing. Defendant has invoked a Fifth Amendment right not to testify. JA406-407.

1. Dorozhko opened an online trading account in early October, 2007.

On or about October 4, 2007, Oleksandr Dorozhko, a self-employed Ukrainian national residing in Uzhgorod, Ukraine (JA62, JA64-68), wire transferred $42,500 to Interactive Brokers, LLC (a U.S. registered broker) to open an online trading account. JA451, JA476-480. In his application to open that account, Dorozhko represented that he had an annual net income of approximately $45,000-$50,000 and claimed a net worth of between $100,000-$250,000. JA451, JA468.

2. On the afternoon of October 17, 2007, a hacker obtained nonpublic information that the earnings of IMS, which were scheduled to be released after the market closed that day, would be below analyst consensus estimates.

On October 17, 2007, IMS Health Incorporated ("IMS"), a public company headquartered in Norwalk, Connecticut, prepared to announce its third quarter earnings results at 5:00p.m. (after the close of the trading markets) that day. JA586-587. Those earnings were well below analyst consensus estimates, and there were no media/analyst reports at the time anticipating negative earnings. JA573, JA587. For several years, Thomson Financial has "hosted" IMS's investor relations website and provided

secure webcasting and audiocasting services for IMS's public release of earnings information, including the October 17th announcement. JA482-83, JA840-841. IMS and Thomson Financial took substantial steps to maintain the confidentiality of the earnings information prior to its public release. JA587-589, JA841-842.

As early as on October 9, several days prior to the October 17 announcement, IMS publicly disclosed that it would announce its third quarter earnings on October 17th at 5:00p.m. (EST) on the IMS website at Thomson Financial. JA851-852, JA939. Thomson Financial had elaborate multi-layered procedures in place to block pre-release access to information such as IMS's third quarter results by anyone except authorized IMS and Thomson Financial personnel. JA841-842, JA847-848.

Beginning at 8:06a.m. (EST) on October 17, a computer hacker from Internet Protocol address ("IP address") 83.98.156.219 began probing the IMS website at Thomson Financial.[2] JA845-846. Because Thomson Financial had not yet received any IMS information, the hacker did not

[2] An "IP address" is a number assigned to a computer. *See* JA853-854.

obtain any confidential IMS information. JA846-847. Three times thereafter, at 12:10p.m., at 12:51p.m., and at 1:52p.m., a computer user from the same IP address probed to determine if Thomson Financial had received the nonpublic IMS information, which it had not. JA845-847, JA908.

At 2:01p.m. on October 17, IMS sent Thomson Financial slides with the third quarter IMS earnings report for the 5:00p.m. conference call and webcast. JA588. After receiving the slides, Thomson Financial transformed them into a proprietary format and uploaded them to an internal secure server. JA843-844. IMS and Thomson Financial expected, and had established procedures to ensure, that the slides would remain confidential until publicly released. JA586-88, JA841, JA843-844.

At 2:15.01 p.m., minutes after the slides had been uploaded, the computer hacker from IP address 83.98.156.219 again probed the Thomson Financial computer network and discovered that Thomson Financial had the IMS information. JA847-848, JA908. Within 27 seconds, starting at 2:15:28 p.m., the hacker breached the Thomson Financial security system and gained access to the confidential IMS information. *Id.* By 2:18.43 p.m.,

the hacker had viewed and/or downloaded all the IMS earnings information. *Id.*

3. Barely a half hour after the hacker obtained the IMS earnings information, Dorozhko spent approximately a year's income buying put options that would become worthless in two days unless the price of IMS stock dropped substantially.

Starting at 2:52p.m. on October 17, barely a half hour after the hacker obtained the confidential IMS information, Dorozhko began using his Interactive Brokers account for the first time in a very aggressive campaign to purchase put options on IMS shares.[3] JA453-463, JA476-553. By 3:06p.m. on October 17, Dorozhko had purchased 300 IMS October put options with a strike price of $25.00 and 330 IMS October put options with a strike price of $30.00. *Id.*

These options were extremely risky. The options expired only two days after Dorozhko purchased them and would have been worthless unless

[3]A put option is a contract that provides the buyer with the right, but not the obligation, to sell a security by a date (the "expiration date") for a certain price (the "strike price"). The buyer of a put option generally expects the market price of the underlying security will decline, allowing the buyer of the option to make a profit from the difference between the strike price (less the cost of the option) and the lower market price. JA571.

IMS stock took a dramatic fall. JA572. This was a substantial purchase for Dorozhko; the investment of $41,670.90 was nearly all the money available in his account, and was nearly equivalent to his income for one year and one-fifth his net worth. JA468, JA487. Dorozhko's purchases were also exceptional in comparison to the market; they represented almost 90% of all IMS October $25.00 and October $30.00 put options purchased between September 4, 2007, and October 17, 2007. JA573.

4. Following release of the earnings results, IMS stock fell 28% and Dorozhko sold the put options for a net profit of over $285,000 – an over 600% return in less than one day.

IMS's stock closed on October 17 at $29.56 per share and the trading volume was 832,500 shares. JA573. Ahead of the conference call and webcast, at 4:33p.m. IMS reported third quarter earnings of 29 cents per share, which was 28% below the analysts' consensus estimates of approximately 40 cents per share and 15% below the previous year's third quarter earnings of 34 cents per share. JA573, JA577-579.

When the markets opened the following day, October 18, 2007, IMS's stock price plunged 28% to a low of $21.20 per share—the steepest decline in the stock's 52-week trading history. JA573. Within six minutes,

Dorozhko had sold all of the 630 IMS put options that he had purchased the previous day, realizing proceeds of $328,571.00 and net profits of $286,456.59. JA451-463, JA477-480. Almost immediately, Dorozhko's broker froze his account. JA463.

C. Course of the proceedings in the district court

On October 29, 2007, based on the investigation it had been able to do in the short time since the trading, the Commission filed a complaint charging Dorozhko with violating Section 10(b) and Rule 10b-5 by gaining access to material nonpublic information regarding IMS's third quarter earnings through fraudulent devices, schemes or artifices. JA9-10. These devices, schemes or artifices were alleged to possibly have included, but were not limited to, hacking into computer networks or otherwise improperly obtaining electronic access to systems that contained confidential information about IMS's imminent earnings release. *Id.* [4]

The complaint was accompanied by an emergency application for a temporary restraining order, an order freezing assets and granting other

[4]A more detailed description of Dorozhko's alleged misconduct is set forth at JA12-15.

relief, and an order to show cause why a preliminary injunction should not issue. JA18-120. On October 30, the district court granted the requested emergency relief, including an asset freeze in the amount of $1,145,826.36, representing the alleged ill-gotten gains plus three times the amount of those gains to cover a possible civil penalty. JA18-26. (The only assets of which the Commission is aware that are subject to the freeze are the proceeds at the broker from Dorozhko's fraud.)

By stipulation of the parties, the temporary restraining order, including the asset freeze, was kept in place until November 28, at which time the court scheduled a hearing into whether a preliminary injunction should issue. JA689-691. In the meantime, defendant filed a motion to dismiss the complaint (JA121-148), and the parties filed briefs addressing the dismissal motion, and the appropriateness of the preliminary injunction and asset freeze.

The hearing was held as scheduled, and the Commission introduced evidence in support of its motion for preliminary injunction, after which the court heard the argument of the parties. JA830-893. The parties then filed post-hearing briefs addressing the question of whether hacking to

obtain nonpublic material information constitutes deception in connection with the sale of securities. JA891.

On January 8, 2008, the district court entered an order denying the Commission's request for a preliminary injunction. JA998-1051. The court found that the Commission had made a sufficient showing that Dorozhko had acquired IMS's earnings information by hacking Thomson Financial's computer system and that he had traded based on that information. JA999-1000. The court further held that the Commission had made a sufficient showing that the alleged hacking and trading constituted a "device or contrivance" as those terms are used in Section 10(b) of the Exchange Act (JA1013), and that his scheme was in connection with the purchase or sale of securities as required by that Section (JA1013-1014). The district court also found that the Commission would suffer irreparable harm if the preliminary injunction was not granted because the funds could move offshore and "it is unlikely that the SEC will be able to recapture" them. JA1009-1010. However, the court concluded that every fraud claim under Section 10(b) requires proof of a breach of fiduciary duty or similar duty of trust and confidence, and that the Commission was

unlikely to prevail on the merits of its claim because it had not alleged that Dorozhko owed IMS or Thomson Financial any fiduciary duty or other duty of trust and confidence. JA1016-1018.

The court therefore denied the preliminary injunction and also ordered that the asset freeze be dissolved, but gave the Commission until January 14 to seek a stay pending appeal in this Court. JA1049-1050. The Commission so moved, and after briefing and argument, this Court ordered the stay to be maintained until the appeal is decided. JA1171.

SUMMARY OF ARGUMENT

This case presents the important issue of whether hacking into a computer system in order to obtain confidential information ordinarily used in trading securities violates the general antifraud provisions of the Exchange Act, Section 10(b) of the Exchange Act and Rule 10b-5 thereunder, which prohibit deceptive devices and contrivances. In the district court, Dorozhko made two arguments as to why it does not: first, that hacking is not deceptive, and second, that no conduct is deceptive within the meaning of the Act unless accompanied by a breach of fiduciary or similar duty. Relying on traditional insider trading decisions where the

fraud occurred when the defendant traded rather than when he obtained the confidential information, the district court agreed with the second argument, concluding that a breach of duty is required in all Section 10(b) violations. This brief demonstrates that both arguments are incorrect.

1. Section 10(b) of the Exchange Act prohibits the employment of "any . . . deceptive device or contrivance" in connection with the purchase or sale of securities that violates Commission rules, and the Commission has adopted Rule 10b-5, which broadly prohibits fraud and deception. "Deception," based on the ordinary meaning of the term, includes any declaration, artifice or practice having the power to mislead, to cause to believe the false, or to disbelieve the true, as by falsification, concealment, or cheating; an attempt to lead into error; a trick or a fraud. "Device or contrivance" includes any scheme to defraud. Dorozhko employed a deceptive device or contrivance when he hacked into a secure computer system to obtain confidential information which he then used to trade securities – he caused the computer system to treat him as though he were authorized to have access to the information when he was not.

2. In a traditional insider trading case, the securities fraud consists not in how the defendant obtains nonpublic information, but in the buying or selling of securities based on nonpublic information in breach of a duty to either refrain from trading or to disclose the intention to trade. In this case, in contrast, the fraud in this case arises from the fact that Dorozhko obtained the information through deceptive means. No breach of duty is required when the defendant engages in affirmatively deceptive conduct, such as lying, acting deceptively, or telling half truths.

ARGUMENT

The sole ground given by the district court for denying a preliminary injunction against future violations and for dissolving the asset freeze was a legal conclusion, namely that conduct can be "deceptive" under Section 10(b) only if it involves a breach of a fiduciary or similar duty. JA1016-1018; *see also*, JA1078-1159. This rule of law, if adopted generally by the courts, would work a revolution in the antifraud provisions of the Exchange Act because it would mean that buyers and sellers of securities and others could lie with impunity so long as they did not owe a pre-existing duty to the targets of their lies.

In this brief, after first stating the applicable standards of review, we show that computer hacking to obtain confidential information is a "deceptive device or contrivance." The defendant argued to the contrary below and is likely to renew the argument on appeal. We then demonstrate that misrepresentations, including false statements, deceptive conduct, or half-truths that render statements that were made misleading, are "deceptive" even if the defendant does not commit a breach of duty when he makes the misrepresentation.

Because the district court's decision rested on a mistaken view of the law, the case should be remanded so that the court may consider whether a preliminary injunction should be granted under the correct legal standards. The asset freeze should be maintained in the meantime.

I. Standards of review for preliminary injunctions against future violations and for prejudgment asset freezes.

This Court reviews a district court's decision to grant or deny a preliminary injunction for abuse of discretion. *SEC v. Cavanagh*, 155 F.3d 129, 131 (2d Cir. 1998) (injunction granted). A district court's decision should be upheld unless it applies legal standards incorrectly or relies upon clearly erroneous findings of fact. *Id.* A lesser showing is required to

justify a prejudgment asset freeze than for a preliminary injunction against future violations. Thus, in *SEC v. Unifund SAL*, 910 F.2d 1028 (2d Cir. 1990), this Court vacated an injunction against future violations but upheld an asset freeze.

A. Injunction against future violations. A preliminary injunction against a violation of the securities laws is appropriate if the Commission makes a substantial showing of likelihood of success as to a current violation and the risk of repetition. *Cavanagh,* 155 F.3d at 131. Unlike a private litigant, the Commission need not show risk of irreparable injury. *Id.*

B. Asset freeze. In explaining why an asset freeze requires a lesser showing of likelihood of success than an injunction against future violations, this Court noted that "the degree to which the Commission must show likelihood of success will be reduced where the interim relief sought is not especially onerous." *Unifund SAL,* 910 F.2d at 1040. An asset freeze is intended to facilitate enforcement of any eventual money judgment by assuring that any funds that may become due can be collected, and it does not place a defendant at risk of contempt for

subsequent securities law violations. *Id.* As an ancillary remedy, it may be granted "even in circumstances where the elements required to support a traditional SEC injunction have not been established," and such a remedy is especially warranted where it is sought for a limited duration. *Id.*

The Court upheld the freeze in *Unifund SAL,* even though it denied a preliminary injunction because the Commission had not yet been able to make a sufficient showing on one of the elements of its case. *Unifund SAL* was an insider trading case where the Court found that the Commission had sufficiently established "a basis to infer appellants traded on inside information," but had not demonstrated that appellants were tipped in violation of a fiduciary duty, which was an element of the claim at issue in that case. The Court ruled that the freeze should be kept in place in order to preserve the Commission's opportunity to collect funds that might yet be ordered paid while it was endeavoring to prove this element at trial. *Id. See also Cavanagh,* 155 F.3d at 131 (in contrast to showing required for injunction against future violations, Commission need only show a likelihood of success on the merits to obtain asset freeze).

II. Dorozhko employed a "deceptive device or contrivance" within the meaning of Section 10(b) when he hacked into a secure computer in order to obtain material nonpublic information.

Section 10(b) declares it unlawful "[t]o use or employ, in connection with the purchase or sale of any security * * * *any* manipulative or *deceptive device or contrivance* in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors." 15 U.S.C. 78j(b) (emphasis added). Rule 10b-5 broadly prohibits fraud and deceit in connection with the purchase and sale of securities.[5] 17 C.F.R. 240.10b-5.

Given the expansive wording of the Rule, the pivotal issue in this case is whether Dorozhko's conduct constituted a deceptive device or contrivance

---

[5] Rule 10b-5 provides:

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

(a) To employ any device, scheme, or artifice to defraud,

(b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or

(c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

within the meaning of the statute. *See Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 213-14 (1976) (scope of the Rule cannot exceed the scope of Section 10(b)). We believe that Dorozhko's conduct did fall within the statutory prohibition because (a) the ordinary meaning of the terms "any ... deceptive device or contrivance" reaches this type of conduct; (b) this type of conduct is considered deceptive or fraudulent under the Computer Fraud and Abuse Act and under other statutes; and (c) Congress intended Section 10(b) to be applied to new types of fraudulent schemes that threaten market integrity and investor confidence.

A. Dorozhko's hacking constituted the employment of a "deceptive device or contrivance."

1. "Any deceptive device or contrivance" is a broad-reaching phrase that covers all schemes to mislead, or to cause to believe the false, such as by trick, falsification, concealment, or cheating.

"We start, as always, with the language of the statute." *Knight v. Commissioner of Internal Revenue,* 128 S. Ct. 782, 787 (2008); *accord, Hochfelder*, 425 U.S. at 197. "In interpreting statutory texts courts use the ordinary meaning of terms unless context requires a different result." *Gonzales v. Carhart*, 127 S. Ct. 1610, 1630 (2007); *Hochfelder,* 425 U.S. at 198

("commonly accepted meaning").[6] Dictionaries used at the time of drafting and enactment of a statute are typically used to provide guidance as to the ordinary meaning of statutory terms. *See Amoco Production Co. v. Southern Ute Indian Tribe*, 526 U.S. 865, 874 (1999); *Austin v. United States*, 509 U.S. 602, 614 n. 7 (1993).

The first relevant term is "any." The Supreme Court has recently explained that "read naturally, the word 'any' has an expansive meaning, that is, one or some indiscriminately of whatever kind." *Ali v. Federal Bureau of Prisons,* 128 S. Ct. 831, 835-36 (2008), *quoting United States v. Gonzalez,* 520 U.S. 1, 5 (1997) *quoting* Webster's Third New International Dictionary 97 (1976). Thus, Section 10(b) should be construed to apply to all "deceptive device[s] or contrivance[s]." *See*, *e.g.*, *id.*; *Affiliated Ute Citizens of Utah v. United States,* 406 U.S. 128, 151 (1972) (the antifraud provisions, "by statute and rule, are broad and, by repeated use of the word 'any,' are obviously meant to be inclusive").

---

[6] *See also*, *Gollust v. Mendell*, 501 U.S. 115, 124 (1991) ("commonly understood"); *Pinter v. Dahl*, 486 U.S. 622, 642-43 (1988) ("common parlance"); *International Brotherhood of Teamsters v. Daniel*, 439 U.S. 551, 559 (1979) ("commonly held understanding"); *SEC v. Variable Annuity Life Ins. Co.*, 359 U.S. 65, 71-73 (1959) ("popular understanding and usage").

For the ordinary meaning of "deceptive device or contrivance," we turn to Webster's International Dictionary (2d ed. 1934), the same dictionary used by the Supreme Court to define the key terms in *Hochfelder*. *See* 425 U.S. at 199 nn. 20, 21 ("device," "contrivance," and "manipulative"); *see also*, *In re Parmalat Securities Litigation,* 376 F. Supp. 2d 472, 502 (S.D.N.Y. 2005) ("deceptive").

These terms have broad, overlapping definitions: "Deceptive" describes any declaration, artifice or practice having the power to mislead, to cause to believe the false, or to disbelieve the true, as by falsification, concealment, or cheating; an attempt to lead into error; a trick or a fraud.[7]

[7] "Deceptive" means "[t]ending to deceive, having power to mislead, as a deceptive appearance." "Deceive" means "[t]o cause to believe the false, or to disbelieve the true." "Deceit" is the "[a]ct of deceiving, as by falsification, concealment, or cheating; deception; An attempt to deceive or lead into error; any declaration, artifice, or practice, which misleads another, or causes him to believe what is false; a wily device; a trick; a fraud. Law Any trick, collusion, contrivance, false representation, or underhand practice, used to defraud another." Webster's International Dictionary 679 (2d ed. 1934).

"Device" and "contrivance" refer to all sorts of schemes to deceive. [8]

Moreover, a "deceptive device or contrivance" is not limited to oral and written statements. As the Supreme Court recently confirmed, "[c]onduct itself can be deceptive." *See Stoneridge Investment Partners v. Scientific-Atlanta, Inc.*, 128 S. Ct. 761, 769 (2008); *see also, id.* at 775 (Stevens, J., dissenting) ("The Court correctly explains why the statute [10(b)] covers nonverbal as well as verbal deceptive conduct.").

2. Dorozhko's conduct in hacking into a secure computer system to obtain nonpublic information was a "deceptive device or contrivance."

"Hacking," the "circumvention of code-based restrictions on computer privileges," occurs in two ways. *See* Orin S. Kerr, *Interpreting "Access" and "Authorization in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1644-45 (Nov. 2003). Hackers either (1) "engage in false identification and

---

[8] As the Court noted in *Hochfelder*, "device" is "[t]hat which is devised, or formed by design; a contrivance; an invention; project; scheme; often, a scheme to deceive; a stratagem; an artifice." 25 U.S. at 199 n. 20 (quoting Webster's International Dictionary 580, 713 (2d ed. 1934). "Contrivance" means "[a] thing contrived or used in contriving; a scheme, plan or artifice," and "contrive" means "[t]o devise; to plan; to plot * * * [t]o fabricate * * * design; invent * * * to scheme * * *." *Id*. (quoting Webster's International Dictionary 580 (2d ed. 1934)).

masquerade as another user who has greater privileges," *e.g.*, "the user can use another person's password, and trick the computer to grant the user greater privileges that are supposed to be reserved for the true account holder," or (2) "exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges." *Id.* at 1645. "Both cases resemble fraud in the factum because the computer does not recognize that it is consenting to access by that particular user. The fraud in the factum voids the authorization, and the access is legally 'without authorization.'" *Id.* at 1655.

The deceptive nature of hacking has led a leading scholar of the securities laws to conclude that a person who tricks another into divulging material nonpublic information, whether by deceptive face-to-face conduct *or by hacking into a computer system,* commits securities fraud. *See* Donald C. Langevoort, 18 *Insider Trading: Regulation, Enforcement, and Prevention,* Section 6:14 (2007).

Computer hacking is no less deceptive simply because the hacker uses the internet to communicate his misleading conduct, or because that conduct is directed at obtaining confidential information that is stored on a

computer. Rather, companies increasingly use computers to perform tasks that once would have been carried out by human beings, such as granting and denying access to confidential information. The ultimate target of the deception is the company that owns the information, and the fact that deception is communicated through a computer system is of no legal consequence.[9]

Turning from these general statements about hacking to the specifics of Dorozhko's misconduct, we find that his easily fits within the definition of "deceptive device or contrivance." Not all of the details of how Dorozhko accomplished his hack are known at this time as Dorozhko invoked a Fifth

---

[9] Some courts have analyzed this issue in terms of the computer being the agent of the deceived party. *See Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1567-68 (1996) (affirming fraud judgment based on unauthorized access to long distance codes, noting that while "no human at Thrifty-Tel received and acted on the misrepresentation," the "reliance by an agent may be imputed to the principal" and "[w]e view Thrifty-Tel's computerized network as an agent or legal equivalent"); *United States v. Flowerday*, 28 M.J. 705, 707-09 (A.F.C.M.R. 1989) (rejecting claim that defendant had not obtained telephone services under false pretenses because he had dialed the number directly without dealing with an operator, court explained that there is no legal significance in the difference between an operator who performs certain actions and an electronic device programmed to perform those same functions because in either case the telephone company programs its human or mechanical agent to recognize and respond to specified conditions).

Amendment right not to testify (JA406-407), he concealed his exit from the computer system (*infra* at 27-28), and some of the details of his hacking were not fully explored due to concerns about trade secrets (JA833).

Despite these limitations in the record, the district court conducted a hearing that elicited sufficient evidence from Thomson Financial's chief information security officer to establish that Dorozkho's hacking was deceptive because he employed deceit to (1) gain unauthorized access to secured nonpublic information, (2) retrieve the information as if he were an authorized recipient, and (3) secretly depart from the compromised computer system.

Furthermore, to the extent that uncertainties in the record are caused by Dorozhko's invocation of the Fifth Amendment, a court is permitted to draw adverse inferences. *See Mitchell v. United States*, 526 U.S. 314, 328 (1999) ("This Court has recognized 'the prevailing rule that the Fifth Amendment does not forbid adverse inferences against parties to civil actions when they refuse to testify in response to probative evidence offered against them.'") (quoting *Baxter v. Palmigiano*, 425 U.S. 308, 318 (1976)); *Collazos v. United States*, 368 F.3d 190, 203-04 (2d Cir. 2004) (noting

that where the defendant "deprives the government of the opportunity to conduct a deposition," that "itself supports an adverse inference as to the criminal source and use of the seized currency."); *SEC v. Brennan*, 230 F.3d 65, 76-77 & n.1 (2d Cir. 2000) (holding that invocation of Fifth Amendment permits adverse inferences).

First, Dorozhko employed hacking as a deceptive trick to gain access to nonpublic information as if he were one of those few persons authorized to have that access. Access to the information was restricted through a sophisticated computer security system to representatives of IMS or Thomson Financial — persons who had a role in either the creation or lawful distribution of that valuable information. JA847-848, JA841-842. To overcome these electronic barriers, the district court noted, Dorozhko used an IP address that was registered in the Netherlands, but that could be used by Dorozhko while he was anywhere in the world due to a "*location-hiding technique* called 'spoofing.'" JA1005 (emphasis added); *see also* JA854 (explaining that "'[s]poofing' is a technique that hackers use to make their traffic look like it's coming from a different IP address"). Dorozkho probed the website at Thomson Financial in an attempt to gain

unauthorized access in order to obtain the nonpublic information. JA846-847. Indeed, Dorozkho tried to obtain unauthorized access to the secured computer system "three times" in an "attempt[] to access the information." JA1005-1006; JA845-847.

Using a hacking device, Dorozkho was eventually able to "breach Thomson Financial's security system." JA-1006. Once access was gained, he continued his deceptive activity by viewing and downloading the slides containing nonpublic information one-by-one as if he were an authorized recipient of the information. *Id.*; *see also*, JA847-848, JA851.

Finally, Dorozkho's egress was also fraudulently accomplished. It took days even to detect that the computer system was compromised. JA848. Although there is, in the district court's words, "powerful" evidence that ties Dorozkho to this deceptive handiwork, his retreat from the security system was so surreptitious that all of the tracks of his fraud have not been completely traced to date, and may never be. JA1007 ("the hacker's IP

address has not been traced at this stage").[10] In sum, Dorozkho employed hacking deceptively to enter, plunder, and abscond.

B. Conduct similar to Dorozhko's is deemed fraudulent or deceptive under other antifraud statutes.

Dorozhko concedes that "a person who trades through fraud but not in violation of a fiduciary duty can be prosecuted for federal crimes, such as computer, mail, or wire fraud." JA1090 (citing JA1001-1002). What he fails to recognize is that the concepts of fraud and deceit in other statutes rely on the same "common understanding" of those terms as does Section 10(b). Thus, it is not surprising to find that courts have reached the sound conclusion that someone who deceptively obtains access to confidential

---

[10] *See*, *e.g.*, *SEC v. Warde*, 151 F.3d 42, 49 (2d Cir. 1998) (affirming jury verdict on 10(b) where evidence that the defendant "intended to conceal" his "deceptive trading practices" was "consistent with, and *admissible to demonstrate*" his liability) (emphasis added); *United States v. Berger*, 473 F.3d 1080, 1085 (9th Cir. 2007) (affirming jury verdict on Section 10(b) claim where part of the defendant's deception was "to conceal the fraudulent nature" of financial misstatements); *United States v. Autunoff*, 1 F.3d 1112, 1115-1117 (10th Cir. 1993) (same).

information stored in a computer has engaged in fraud or deceit. [11] Relevant decisions include (a) the two *Cherif* decisions from the Seventh Circuit, one a Commission case under Section 10(b) and the other a criminal conviction under the mail and wire fraud statute; (b) decisions under the Computer Fraud and Abuse Act; and (c) decisions under other provisions of the law.

1. The two *Cherif* decisions find that unauthorized electronic access for the purpose of obtaining confidential information is a form of fraud under both Section 10(b) and the mail fraud statute.

Danny Cherif devised a "simple, cunning scheme" to obtain confidential information that he could use to place profitable securities trades. *SEC v. Cherif,* 933 F.2d 403, 406 (7th Cir. 1991). After Cherif's employment at a bank was terminated, he continued to use his magnetic identification card to enter the bank building, despite an electronic security system that restricted access to the building to current employees. After

[11] As the quotation from his Stay Opp. suggests (JA1090), the only distinction Dorozhko has offered between these other statutes and Section 10(b) is his assertion that all Section 10(b) claims require proof of breach of a fiduciary duty in addition to a deceptive act. We show that this breach-of-duty argument is without merit in the next section of this brief.

entry, he went to a department of the bank that kept information about upcoming corporate transactions. He traded securities based on some of the nonpublic material information he found there. The Commission sued him for violating Section 10(b) and Rule 10b-5, *SEC v. Cherif,* 933 F.2d 403, and he was also indicted and convicted for mail and wire fraud, *United States v. Cherif*, 943 F.2d 692 (7th Cir. 1991). In both cases the court found that his conduct was fraudulent under the "common understanding" of that term, looking specifically to Supreme Court decisions construing the mail fraud statute for that understanding.

The district court in the Commission's case granted a preliminary injunction against future violations and an asset freeze. Cherif appealed on the ground that he had not committed securities fraud. In affirming the district court's decision, the court of appeals observed that Cherif's actions were "fraudulent in the *common understanding* of the word because they deprived some person of something of value by trick, deceit, chicane or overreaching." 933 F.2d 403, 411-12 (7th Cir. 1991) (emphasis added),

quoting decisions under the mail fraud statute, including *McNally v. United States*, 483 U.S. 350, 358 (1987).[12]

The court of appeals also affirmed Cherif's mail and wire fraud convictions.[13] Cherif claimed that he had "obtained the bank's information by trespass or burglary, not by fraud." *United States v. Cherif*, 943 F.2d at 696. The court of appeals responded that "[t]his contention cannot be serious" because, among other fraudulent acts, "every time he used the keycard Cherif, in effect, falsely represented that he was a bank employee

---

[12] The decision in the Commission's case against Cherif ultimately turned on the court's conclusion that Cherif continued to owe a fiduciary duty to the bank even after his employment terminated, so that he was liable for insider trading under the misappropriation theory, which requires proof that defendant breached a duty of disclosure. 933 F.2d at 411. The court therefore did not have to reach the question of whether the fraudulent entry alone could have been a basis for finding a violation of Section 10(b) in the absence of that duty, but this fact does not change the court's express statement that the conduct was fraudulent in the "common understanding."

[13] These statutes make it a crime for a person who "having devised . . . a scheme or artifice to defraud or obtain money or property by means of false or fraudulent pretenses, representations, or promises" to use the mail or wires "for the purpose of executing the scheme." 943 F.2d at 695. The indictment alleged that Cherif devised a scheme to defraud the bank and its clients of confidential information by reactivating his identification card and using it to enter the bank to obtain the information, and then using the information to obtain money by trading securities. *Id.*

entitled to be in the bank." *Id*. The court explained that the "common understanding" of "to defraud" in the mail fraud statute is "wronging one in his property rights by dishonest methods or schemes."[14]

By tricking Thomson Financial's computer system into providing him IMS's nonpublic information as if he were one of those few persons entitled to access such information, Dorozhko likewise committed fraud. In other words, Cherif hacked into a building and Dorozkho hacked into a computer system; both violated Section 10(b) by gaining, through trickery, unauthorized access to nonpublic information for the purpose of trading.

2. Gaining unauthorized access to a computer system for the purpose of obtaining confidential information is a form of fraud under the Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act (CFAA) addresses "[f]raud and related activity in connection with computers." Section 1030(a)(4) of the CFAA provides that whoever "knowingly and *with intent to defraud*, accesses" a computer covered by the Act "without authorization, or

[14] The court's statement of the "common understanding" of "to defraud" quotes a different phrase in the same sentence from *McNally* that the court quoted in defining "fraud" in the Commission's case.

exceeds authorized access, and by means of such conduct *furthers the intended fraud* and obtains anything of value" shall be punished as provided in the Act. *See* 18 U.S.C. 1030(a)(4) (emphasis added). Courts have readily applied this statute to remedy unauthorized access to obtain confidential information.

For example, in *Creative Computing* the Ninth Circuit affirmed a jury verdict and permanent injunction under the CFAA where the officers of a trucking company "hacked into the code [that a rival trucking company] used to operate its website," "examined the source code," and obtained access to its competitor's "tremendously valuable" data. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 932 (9th Cir. 2004). Defendants also successfully guessed login names and passwords that enabled them to gain access to the information. The court described this conduct as "in effect impersonating the trucking company to sneak into" the other company's website. 386 F.3d at 932. "These tricks enabled [defendants] to see all of the information available to [the other company's] bona fide customers." *Id.* On appeal, the defendant did not challenge the finding that its conduct violated Section 1030(a)(4), but instead only

claimed that plaintiff's injury did not meet the statutory jurisdictional amount.[15]

3. Hacking, including hacking to obtain access to confidential information, is also a form of fraud under legal provisions other than the CFAA.

Courts also do not hesitate to conclude that computer "hacking" is a form of fraudulent deception outside the CFAA context. For example, in *United States v. Riggs,* 739 F. Supp. 414, 418-19 (N.D. Ill. 1990), the district court refused to dismiss an indictment alleging that the defendant committed wire fraud when he participated in a scheme to hack into a phone company computer in order to obtain confidential information,

[15] Other cases in which defendants who hacked into computer systems in order to obtain confidential information were convicted under Section 1030(a)(4) include: *United States v. Peterson*, 98 F.3d 502, 504 (9th Cir. 1996) (affirming defendant's sentence under Section 1030(a)(4) where the defendant hacked into a consumer credit reporting agency to obtain information that he used to order credit cards); *United States v. Sykes*, 4 F.3d 697 (8th Cir. 1993) (*per curiam*) (affirming sentence for violation of Section 1030(a)(4) for unauthorized use of an automatic teller machine card and personal identification number); *see also*, *United States v. Ivanov*, 175 F. Supp. 2d 367, 371-72 (D. Conn. 2001) (denying motion to dismiss indictment under Section 1030(a)(4) where Russian national hacked into retail transaction clearinghouse's computer and obtained credit card data).

ruling that the hacking constituted a "fraudulent means" of accessing the computer.

Courts adjudge hacking to be deceptive using traditional – not innovative – legal principles. When a hacker penetrates a system that was designed to provide access to confidential information to a limited set of authorized individuals, he misrepresents his identity and authority. *See*, *e.g.*, *United States v. Miller*, 70 F.3d 1353, 1355 (D.C. Cir. 1995) ("Each time Miller inserted Rolark's card into an ATM and entered her personal four-digit code, he represented to [the bank] that he had authority to withdraw funds from Rolark's account"); *Thrifty-Tel*, 46 Cal. App. 4th at 1567 (affirming civil fraud judgment, where the fraud cause of action "applies a hoary common law theory to computer-age facts," namely that defendants' "use of the confidential access code was the legal equivalent of a misrepresentation that they were authorized users of its services, and plaintiff relied to its detriment on that misrepresentation when its computer automatically granted them access to the network"); *State v. Hamm*, 569 S.W.2d 289, 290-91 (Mo. Ct. App. 1978) (by using someone else's ATM card, "defendant represented falsely that he did have authority

to use the" card). Likewise, access to the nonpublic information here was restricted by Thomson Financial to authorized individuals (JA1006, JA848), and in accessing and using that information Dorozhko falsely represented that he possessed such authorization.

C. Congress intended Section 10(b) to be applied to new types of fraudulent schemes that threaten market integrity and investor confidence.

The district court observed that "in the 74 years since Congress passed the Exchange Act, no federal court has *ever* held that the theft of material nonpublic information by a corporate outsider and subsequent trading on that information violates § 10(b)." JA1000 (emphasis in original), JA1038-1040. The fact that there has not been a previous hacking case litigated under the Exchange Act, however, is not dispositive because both Congress and the Supreme Court have endorsed the view that Section 10(b) should be applied to remedy new forms of fraudulent schemes as

well as the more familiar ones.[16]

For instance, this Court did not recognize its first insider trading case until *SEC v. Texas Gulf Sulphur Co.*, 401 F.2d 833 (2d Cir. 1968), some 34 years after passage of the Exchange Act. The Court did not stop at the fact that there had not been a previous case holding that trading on material, nonpublic information is fraudulent, but instead applied established legal principles to the conduct to find a violation. As this Court has observed in another context, "[t]he fact that there is no litigated fact pattern precisely in point may constitute a tribute to the cupidity and ingenuity of the malefactors involved but hardly provides an escape from [the remedies of] the securities fraud provisions." *United States v. Brown*, 555 F.2d 336, 339-40 (2d Cir. 1977). There have not been previous litigated cases like this one, but this one will likely not be the last.

---

[16] If the district court was suggesting that Dorozhko's conduct was not deceptive because it was a form of theft, it was in error. We have just demonstrated that Dorozhko committed deception, and the mere fact that a deceptive scheme may involve some conduct that would qualify as theft does not deprive the conduct of its deceptive nature. Cf., Model Penal Code § 223.3 (theft by deception).

As the Supreme Court has explained, the legislative history of the Exchange Act makes clear that Section 10(b) is intended to reach all sorts of fraudulent schemes; that history describes the provision as a "catchall" against fraud in its various forms, including newly created types. *Hochfelder,* 425 U.S. at 202, quoting Hearings on H.R. 7852 and H.R. 8720 before the House Committee on Interstate and Foreign Commerce, 73d Cong., 2d Sess., 115 (1934). Thomas Corcoran, the Act's principal drafter, famously emphasized the provision's role as a supplement to the specific prohibitions contained in other sections of the Act by paraphrasing it as "Thou shalt not devise any other cunning devices." *Id.* In short, "Section 10(b) and Rule 10b-5 prohibit all fraudulent schemes in connection with the purchase or sale of securities, whether the artifices employed involve a garden type variety of fraud, or present a unique form of deception," because "[n]ovel or atypical methods should not provide immunity from the securities laws." *Superintendent of Insurance v. Bankers Life & Cas. Co.*, 404 U.S. 6, 11 n.7 (1971) (quoting *A. T. Brod & Co. v. Perlow*, 375 F.2d 393, 397 (2d Cir. 1967)).

Certainly the *harm* caused by Dorozhko's misconduct is not new. Indeed, it is the same sort of harm to market integrity and investor confidence that is caused by trading in breach of a fiduciary duty. The Supreme Court explained this harm when it accepted the misappropriation theory of insider trading liability in *O'Hagan*:

> [a]lthough informational disparity is inevitable in the securities markets, investors likely would hesitate to venture their capital in a market where trading based on misappropriated nonpublic information is unchecked by law. An investor's informational disadvantage vis-à-vis a misappropriator with material, nonpublic information stems from contrivance, not luck; it is a disadvantage that cannot be overcome with research or skill.

United States v. O'Hagan, 521 U.S. 642, 658-59 (1997); *see also*, *United States v. Carpenter*, 791 F.2d 1024, 1030-31 (2d Cir. 1986), *aff'd by equally divided court sub nom.*, *Carpenter v. United States*, 484 U.S. 19 (1987).

O'Hagan involved trading by a lawyer who misappropriated information that had been entrusted to him by trading on it in breach of a fiduciary duty, while Dorozhko used deception in obtaining the information. The danger to the markets is the same in each case – whether a fraudfeasor misappropriates lawfully obtained information or instead deceives the owner of the information into revealing it, his misconduct

threatens investors' confidence, making it less likely that they would venture their capital into the United States securities markets.

The problem only threatens to get worse in the future given that hacking in connection with securities trading is an increasingly common phenomenon. *See, e.g., SEC v. Stummer*, 1:2008CV03671 (DAB) (S.D.N.Y. April 17, 2008) (settled case against alleged computer hacker trading on material nonpublic information); *SEC v. Lohmus Haavel & Viisemann, et al.*, 05 CV 9259 (RWS) (S.D.N.Y. Nov. 1, 2005) (same); *SEC v. Blue Bottle Ltd.*, 07-cv-01380 (CSH) (KNF) (S.D.N.Y. Feb. 26, 2007) (default judgment obtained against alleged computer hackers trading on material nonpublic information). Congress enacted the expansive language of Section 10(b) to reach deceitful schemes known to it in 1934 and those yet to be invented. Applying the statute to Dorozhko's conduct effectuates that Congressional purpose.

III. A lie, trickery, or half-truth is "deceptive" whether or not the person making the misrepresentation is acting in breach of a fiduciary duty.

Dorozhko successfully persuaded the district court that his conduct was not "deceptive" because, he claimed, every violation of Section 10(b)

requires proof of a breach of fiduciary duty, even where the defendant lies, engages in misleading conduct, or tells half-truths, and Dorozhko did not owe a fiduciary duty to IMS or Thomson Financial.[17] Though the district court found that Dorozhko's conduct was a device or contrivance, it agreed that his conduct was not deceptive. After an extensive discussion of the law of insider trading cases, which hold that trading in breach of a fiduciary duty is a form of fraud (JA1018-1049), the court concluded that "a breach of fiduciary duty of disclosure is a required element of *any* 'deceptive' device under § 10(b)" JA1017-1018 (emphasis added). The court looked at traditional insider trading decisions, where the fraud consists not in how the information is obtained, but in the fact that it is used to make securities trades. As we have noted, however, this is not such a case.

It is difficult to overstate the degree to which Dorozhko's argument is both extraordinary and untenable. To take only one striking consequence,

---

[17] He repeated this argument in this Court in opposition to the Commission's motion to maintain the asset freeze pending appeal – "a violation of § 10(b) and Rule 10b-5 necessarily entails a breach of fiduciary or similar duty." JA1097.

under Dorozhko's view the well-known form of fraud known as a "pump-and-dump" – in which fraudfeasors acquire a block of shares in a company, engage in fraudulent conduct to increase the price, and then use a fraudulent sales campaign to sell the stock to unsuspecting strangers before the truth is disclosed – will no longer be subject to Rule 10b-5 except in the unusual situation where the perpetrators of the scheme owe a fiduciary duty to the investors they deceive.

As we discuss in detail below, fraud and deceit under both the common law and the securities laws are governed by well-established principles: A material misrepresentation, which includes false statements, deceptive actions, and half-truths that render statements made misleading, is fraudulent. Silence, on the other hand, is not deceptive unless a duty to speak is created by a fiduciary relationship or other source.

Dorozhko's interpretation would turn these principles on their head. Instead of being a special case that can give rise to a fraud claim even without an affirmative misrepresentation, the existence of a fiduciary duty would be the predicate to all fraud claims, so that even out-and-out lies would not be deemed "deceptive" unless the liar was breaching a duty in

addition to telling lies. The notion that a lie is not deceptive unless it also breaches a duty is contrary to the plain language and legislative history of Section 10(b), to the common law background against which the securities laws were enacted, to existing case law recognizing that a Section 10(b) violation can be based on fraudulent or deceptive acts without a breach of duty, and to good policy.

A. The language and legislative history of Section 10(b) establish that it reaches all deceptive devices and contrivances, with no requirement of a breach of duty.

We have already discussed the breadth of the language of Section 10(b), and its legislative history, which refers to the provision as a "catchall" and as a prohibition on all cunning schemes, whether new or old. *Supra* at 19-22, 36-40. The notion that what Congress really meant when it enacted Section 10(b) is that fiduciaries – who already had a duty to make full disclosure – are the only ones also prohibited from making affirmative misrepresentations, is simply implausible.

B. The Supreme Court has explained that Section 10(b) follows the common law rule that deception may be shown *either* by affirmative misrepresentations *or* by silence in breach of a duty of disclosure.

1. The distinction between fraud through affirmative misrepresentation and fraud through breach of duty is most clearly illustrated in the Court's insider trading cases.

The general rule that misrepresentations are fraudulent, but that silence is fraudulent only if there is a duty to disclose, is clearly explained in the Supreme Court's insider trading cases. The first case in which the Supreme Court recognized that insider trading was a deceptive device or contrivance under Section 10(b) even though the defendant had not made an affirmative misrepresentation was *Chiarella v. United States*, 445 U.S. 222 (1980) . That case involved an employee of a financial printing company who traded securities based on information that he learned in the course of his employment. 445 U.S. at 224. The employee was convicted of violating Section 10(b) and Rule 10b-5, and he appealed to the Supreme Court on the ground that merely trading based on material, nonpublic information was not securities fraud.

The Court observed that the case "concerns the legal effect of the [defendant's] silence." 445 U.S. at 226. To ascertain that effect, it first looked to the language of the statute and the legislative history, but neither of these provided specific guidance as to whether "silence may constitute a manipulative or deceptive device." *Id.*

However, the Court noted, the common law had long held that silence can be fraudulent when the failure to speak breaches a duty to disclose. The Court explained that the Commission, correctly applying common law principles, had held that corporate insiders had "an affirmative duty to disclose material information which has been traditionally imposed on corporate 'insiders,' particularly officers, directors, or controlling stockholders" when they sell securities of the corporation, and that the failure to comply with that disclosure obligation was a violation of Section 10(b). 445 U.S. at 227, *quoting Cady, Roberts & Co.,* 40 S.E.C. 907, 911 (1961). The Commission's conclusion rested on the reasoning of Judge Learned Hand that "the director or officer assumed a fiduciary relation to the buyer by the very sale . . .." 40 S.E.C. at 914 n.23, *quoting Gratz v. Claughton,* 187 F.2d 46, 49 (2d Cir. 1951).

The Supreme Court went on to explain that the Commission's view was well-founded in the common law:

> At common law, *misrepresentation made for the purpose of inducing reliance upon the false statement is fraudulent*. But *one who fails to disclose material information* prior to the consummation of a transaction *commits fraud only when he is under a duty to do so.* And the duty to disclose arises when one party has information "that the other [party] is entitled to know because of a fiduciary or other similar relation of trust and confidence between them."

445 U.S. at 227-28 (emphasis added).

After reviewing court decisions applying this rule in securities cases, the Court concluded that "silence in connection with the purchase or sale of securities may operate as a fraud actionable under Section 10(b)" where there is "a duty to disclose arising from a relationship of trust and confidence between parties to a transaction." 445 U.S. at 230.[18]

Thus, the courts and commentators typically state that the deception element under Section 10(b) and Rule 10b-5 as requiring proof of *either* "a

---

[18] The principle that silence is fraudulent only when there is a duty to disclose has been applied in the Court's subsequent insider trading cases, where the dispositive issue in each case has been whether the defendant owed a duty such that failure to make disclosure violated Section 10(b). *See, e.g., O'Hagan*, 521 U.S. 642 (adopting misappropriation theory of liability).

material misrepresentation *or* a material omission as to which he had a duty to speak." *SEC v. Monarch Funding Corp.,* 192 F.3d 295, 308 (2d Cir. 1999) (emphasis added). *See also* Arnold S. Jacobs, *Disclosure and Remedies Under the Securities Laws Database* Part III, Ch. 12.VII.B (March, 2008) ("While some duty must be owed by the defendant to the plaintiff in complete silence cases, under the duty theory, liability for misrepresentations flows absent a fiduciary or other duty between the plaintiff and the defendant.").

2. The Supreme Court has recognized that fraud may be based on either misrepresentations or failure to speak in violation of a duty in non-insider trading cases as well.

A recent example where the Court recognized that fraud can be committed either by misrepresentation or by breach of duty is *Stoneridge*, 128 S. Ct. 761. The issue in that case was whether plaintiffs in a private damages suit could recover from defendants who had allegedly participated in arrangements that allowed a securities issuer to mislead its auditor and issue misleading financial statements affecting its stock price, but who had no role in preparing or disseminating the financial statement. The Court ultimately held that plaintiffs could not recover from these

defendants because plaintiffs had not relied on defendants' statements or representations.

In the course of reaching that conclusion, the Court reviewed the causation requirements for a private right of action under Section 10(b). It explained that proof of reliance on the defendant's "deceptive acts" is ordinarily required, but that reliance may be presumed in two situations, one where the fraud involves failure to disclose in breach of a duty, and where the defendant has made an affirmative misstatement. The first presumption arises "if there is an omission of a material fact by one with a duty to disclose," while the second is present in a case governed by the "fraud-on-the-market" doctrine, "when the statements at issue become public." Neither presumption applied in *Stoneridge* – the first because defendant "had no duty to disclose" and the second because defendants "deceptive acts were not communicated to the public." 128 S.Ct. at 769.

Thus, the Court clearly recognized that duty is not required in cases where there has been affirmatively deceptive conduct – if a duty to disclose were always an element of a Section 10(b) case, there would have been no need to find that the statements had not been communicated to the public

because the case would have been disposed of by the absence of an allegation that defendants owed a duty.

Another case demonstrating that misrepresentations may be the basis for a Section 10(b) claim even without a duty is *Basic Inc. v. Levinson*, 485 U.S. 224, 240 n.18 (1988), where the Court declined to recognize two different standards of materiality, one for "situations where insiders have traded in abrogation of their duty to disclose or abstain" and another covering "affirmative misrepresentations by those under no duty to disclose (but under *the ever-present duty not to mislead*)" (emphasis added). The question whether one or two standards were appropriate would have been meaningless if every Section 10(b) case required proof of breach of duty, even when the defendant has violated the "ever-present duty not to mislead." As in *Stoneridge,* the Court proceeded from the premise that an affirmative deception is a basis for Section 10(b) liability without any breach of duty.

C. This Court has recognized that fraud can violate Section 10(b) even if there is no breach of fiduciary duty.

This Court has reviewed many securities fraud cases, and it has never required proof of a breach of a duty when the defendant has made an

affirmative misrepresentation or engaged in deceptive conduct. *See*, *e.g.*, *In re NYSE Specialists Sec. Litig.*, 503 F.3d 89, 102 (2d Cir. 2007) (holding that Rule 10b-5 reaches misstatements by "bankers and non-issuer sellers"). The issue has not previously come up in the way it does here, perhaps because no one has ever suggested before that an affirmative misrepresentation is not deceptive. But there are at least two areas where this Court has explicitly said that there can be deception under Section 10(b) without breach of duty – pump-and-dump schemes and market manipulations.

1. Pump-and-Dump Schemes. This Court has expressly held in a criminal case that a pump-and-dump scheme violates Section 10(b) and Rule 10b-5 even though defendants did not act in breach of a fiduciary duty. *See United States v. Skelly,* 442 F.3d 94 (2d Cir. 2006). The government's primary theory of liability was that defendants pumped up the price of the securities "and then used fraudulent and high-pressure tactics to unload ('dump') the securities on unsuspecting customers." 442 F.3d at 96. However, the government also offered an alternative theory that the defendants breached a fiduciary duty towards their customers.

Defendants were convicted in a general verdict, and they claimed that their convictions should be reversed because the district court misinstructed the jury on the circumstances under which a fiduciary duty is created.

This Court rejected the challenge. First of all, it noted that breach of duty is relevant in failure to disclose cases, not in affirmative misrepresentation cases: "a seller or middleman may be liable for fraud if he lies to the purchaser or tells him misleading half-truths, but not if he simply fails to disclose information that he is under no obligation to reveal." 442 F.3d at 97. Then it held that any error in the instruction on the government's fiduciary theory duty theory was not prejudicial to defendant because there was ample evidence that defendants engineered a pump-and-dump scheme, and it was overwhelmingly likely that any reasonable jury would have convicted based on that theory. 442 F.3d at 98. In other words, this Court affirmed the verdict on the ground that defendants' affirmative fraudulent conduct was clearly proven, even assuming that the fiduciary duty theory was not properly presented to the jury.

2. Manipulation. A second area where this Court has upheld findings of violations under Section 10(b) without proof of a fiduciary duty is market manipulation, *i.e.*, practices such as wash sales, matched orders, or rigged prices "that are intended to mislead investors by artificially affecting market activity." *ATSI Comm., Inc. v. Shaar Fund, Ltd.,* 493 F.3d 87, 99-100 (2d Cir. 2007). Section 10(b) covers "manipulative" devices and contrivances as well as deceptive ones, while Rule 10b-5 forbids fraudulent and deceitful conduct but does not use the word "manipulative." Manipulation is prohibited by Rule 10b-5 because it involves "intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities." *Id.,* 493 F.3d at 100, *quoting Hochfelder,* 425 U.S. at 199.[19]

For our purposes here, the key conclusion is this Court's statement that Rule 10b-5 forbids market manipulation, which is a form of deception,

---

[19] Indeed, this Court requires "a showing that an alleged manipulator engaged in market activity aimed at deceiving investors as to how other market participants have valued a security," deception that arises from the fact that "investors are misled to believe that prices at which they purchase and sell securities are determined by the natural interplay of supply and demand, not rigged by manipulators." *ATSI,* 493 F.3d at 100 (internal quotation and citation omitted).

"regardless of whether there is a fiduciary relationship between the transaction participants." *Id.*, 493 F.3d at 101. Thus, manipulation is a second example where this Court has expressly found that deception under Section 10(b) does not require proof of a fiduciary duty.

D. The district court's error was in applying the special rules that govern fraud-through-breach-of-duty-to-disclose, such as in traditional insider trading cases, to a case where there was active deception.

The district court's fundamental error was in analyzing Dorozhko's conduct under theories of liability that apply when a fiduciary, after obtaining information lawfully, trades in breach of a duty to either disclose his intention to trade or to refrain from doing so. *O'Hagan*, 521 U.S. 642 (partner in law firm had non-fraudulent access to confidential client information); *Chiarella*, 445 U.S. 222 (employee of printer had non-fraudulent access to confidential customer information). The fraud in that type of case is "consummated, *not when the fiduciary gains the confidential information*, but when, without disclosure to his principal, he uses the information to purchase or sell securities." *See O'Hagan*, 521 U.S. at 656 (emphasis added); *Chiarella*, 445 U.S. at 227-28. In the present case, in contrast, the fraud was the affirmative conduct by which Dorozhko

deceptively obtained the information. Nothing in the language of the statute imposes a duty requirement when the wrongdoer defrauds through acts of deception rather than by remaining silent.

An argument very similar to Dorozhko's was rejected in *United States v. Riggs,* 739 F. Supp. at 418-19, a case that was discussed above in showing that Dorozhko's conduct was deceptive. *Supra* at 34-35. Like Dorozhko, the defendant in that case claimed that he could not be liable for fraudulently obtaining confidential information because he owed no fiduciary duty to the phone company, the owner of the information. He cited *Dirks v. SEC,* 463 U.S. 646 (1983), one of the Supreme Court's insider trading cases, in support of this assertion. The district court rejected his argument, distinguishing *Dirks* on the ground that in that case the defendant "c[a]me upon information *lawfully*" and then breached a fiduciary duty by trading without making required disclosure, while in the case then before it the defendant had participated in a scheme to fraudulently obtain the information in the first place. *Riggs*, 739 F. Supp. at 419 (original emphasis). This analysis applies equally to Dorozhko.

CONCLUSION

For the foregoing reasons, the district court's denial of a preliminary injunction and its decision to vacate the prejudgment asset freeze should be reversed.

Respectfully submitted.

_____

BRIAN G. CARTWRIGHT
General Counsel

ANDREW N. VOLLMER
Deputy General Counsel

JACOB H. STILLMAN
Solicitor

MARK PENNINGTON
Assistant General Counsel

DAVID LISITZA
Attorney

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-8010
(202) 551-5015 (Lisitza)

May 2008

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C)

I hereby certify that, pursuant to Fed. R. App. P. 32(a)(7)(C), the attached brief is proportionately spaced, has a typeface of 14 points or more, and contains 10,884 words.

Dated: May 6, 2008

_____

David Lisitza
Securities and Exchange Commission
100 F St., N.E.
Washington, D.C. 20549-8010
May 5, 2008
(202) 551-5015

CERTIFICATE OF SERVICE

I hereby certify that, on this day, I caused the original and 10 copies of the foregoing brief and 10 copies of the Appendix to be sent by overnight delivery (as well as one electronic copy) to

Catherine O'Hagan Wolfe
Clerk of Court
U.S. Court of Appeals for the Second Circuit
The Daniel Patrick Moynihan Courthouse
500 Pearl Street
New York, NY 10007

and two copies of the foregoing brief (and one electronic copy) as well as one copy of the Appendix to be sent by overnight delivery

Charles A. Ross, Esq.
Christopher L. Padurano, Esq.
Charles A. Ross & Associates
111 Broadway
Suite 1401
New York, NY 10006
cross@carossassoc.com; cpadurano@carossassoc.com

Dated: May 6, 2008

_____

David Lisitza