LAW FIRM "MOST FEARED" GLOBALLY BY LARGE BUSINESSES
BTI Consulting Group Survey

July 2022

quinn emanuel

quinn emanuel urquhart & sullivan, llp | business litigation report

atlanta | austin | boston | brussels | chicago | doha | hamburg | hong kong | houston | london | los angeles | mannheim | miami | munich | neuilly-la defense
new york | paris | perth | riyadh | salt lake city | san francisco | seattle | shanghai | silicon valley | stuttgart | sydney | tokyo | washington, d.c. | zurich

SEC's Novel Insider Trading Theory Casts Long Shadow

The U.S. Securities and Exchange Commission ("SEC" or "Commission") is advancing a novel insider trading theory known as "shadow trading." *See* Mihir N. Mehta, David M. Reeb, and Wanli Zhao, "*Shadow Trading*," The Accounting Review (July 2021). Individuals who engage in "shadow trading," the theory goes, impermissibly circumvent insider trading restrictions when they use confidential information about one company to make an investment decision about the company's competitors or supply chain partners. The SEC adopted this expansive take on the classical insider trading theory last year in the *Panuwat* case. Since then, the SEC has given signals that *Panuwat* may not be a one-off – the Division of Enforcement and Division of Examinations are actively scrutinizing investment advisors' and individuals' use of confidential information when they place bets on so-called "economically-linked" companies.

In our view, *Panuwat* does not suggest a need to rethink compliance completely. Although the SEC's "shadow trading" theory has the potential to engulf all manner of trading, we suspect the practical application will have a narrower reach. Firms need not immediately set about rewriting their trading policies or increase compliance headcount just yet. In many instances, advisers can address the SEC's concerns by augmenting their existing policies and procedures to encourage internal reporting and probe the reach of potential material nonpublic information ("MNPI"). To do so, firms must understand the "shadow trading" landscape.

The Panuwat: SEC's First "Shadow Trading" Action

The SEC's insider trading charges against Matthew Panuwat marked the agency's first-ever "shadow trading" action. *See SEC Charges Biopharmaceutical Company Employee with Insider Trading*, SEC Litigation Release No. 25170 (Aug. 17, 2021). The SEC alleged that Mr. Panuwat had confidential information about his employer's impending acquisition by a larger company and, on the basis of that information, he purchased out-of-the-money, short-term stock options in one of his employer's competitors—a similarly-sized company in the same industry that was also

(continued on page 2)

INSIDE

Partner Victoria Maroulis Named One of "Top 250 Women in IP" for 2022

Quinn Emanuel Partner Victoria Maroulis was named one of the "Top 250 Women in IP" for 2022 by Managing IP. The list—published annually since 2013—recognizes the industry's leading female intellectual property practitioners in private practice worldwide who have performed exceptionally for their clients and firms in the past year.

Firm Receives Top Rankings in *Legal 500 United States 2022*

The firm ranked in *The Legal 500 United States 2022*, "the Clients' Guide to the best Law firms, Top Lawyers, Attorney, Advocates, Solicitors and Barristers." The firm has been recognized across 24 practice areas, spanning six jurisdictions, with 18 partners individually highlighted for outstanding achievements over the past calendar year.

Firm Receives Top Rankings in *IAM Patent 1000: The World's Leading Patent Professionals*

The firm ranked in the 2022 edition of *IAM Patent 1000: The World's Leading Patent Professionals*. The firm has been recognized in eight jurisdictions, with 21 partners individually highlighted for their exceptional achievements over the past calendar year.

ripe for a business combination (an "economically-linked company" in "shadow trading" parlance). Mr. Panuwat believed the competitor's stock price would jump when news of his employer's acquisition broke. He was right. The competitor's stock went up 8% on the news, and Mr. Panuwat profited roughly $100,000 on his trades.

The SEC alleges that this conduct—trading in securities of a *third party*—constitutes insider trading. They argue that Mr. Panuwat had a duty *not* to trade in a competitor's stock because his employer's insider trading policy prohibited him from using MNPI obtained at work to trade in "the securities of another publicly traded company, including all significant collaborators, customers, partners, suppliers, or competitors of the Company." *See SEC v. Panuwat, 4:21-cv-06322 (N.D. Cal., filed Aug. 17, 2021).* The SEC argues, too, that the information was material with regard to the competitor: various factors tied together the fortunes of the two companies at the time the acquisition was announced, and the information *must have* been material because the competitor's stock price jumped when the merger was announced. (The price went up, the SEC observes, so the venerable "reasonable investor" must have considered news of the merger important in making investment decisions – a kind of securities law *res ipsa*.)

Generally, to prevail in an insider trading case, the SEC must demonstrate that a trader knowingly bought or sold a security, while in possession of MNPI, in breach of a duty of confidence or trust. The SEC's case against Mr. Panuwat raises two critical questions that will shape the "shadow trading" theory: (1) whether an insider trading policy creates a duty of trust that extends to trading in *a competitor's stock*, and (2) whether the nonpublic information Mr. Panuwat possessed was material with respect to *an unrelated third party*.

Unfortunately for firms grappling with the implications of *Panuwat*, those questions remain unresolved. In January, the U.S. District Court for the Northern District of California ruled that the SEC made a sufficient showing to survive a motion to dismiss, extending the case. The Court found that "the SEC's theory of liability falls within the contours of the misappropriation theory and the language of the applicable law," and declined to toss the case simply because the SEC was pursuing a new theory. *See SEC v. Panuwat,* No. 21-CV-06322-WHO, 2022 WL 633306, at *1 (N.D. Cal. Jan. 14, 2022).

Many observers hoped that the Court in *Panuwat* would reject the SEC's novel theory outright or, in the alternative, provide guidance on the reach of the theory. The Court did neither. Thus, the industry is left to grapple with *Panuwat*'s compliance implications, trying to divine which steps are necessary and appropriate, and which are pointless shadow boxing.

EXAMS Focus on Trading in "Similar Industries"

In April, a Divisions of Examinations' ("EXAMS") Risk Alert on "Investment Adviser MNPI Compliance Issues" signaled the SEC's intention to continue looking for instances of "shadow trading." *See* Division of Examinations Risk Alert, "*Investment Adviser MNPI Compliance Issues*" (April 26, 2022). The alert details "notable deficiencies" the EXAMS staff observed during recent examinations of registered investment advisers. Among the deficiencies, the staff noted firms' failure to implement adequate policies and procedures relating to their expert network consultants, including "[r]eviewing relevant trading activity of supervised persons in the securities of publicly traded companies *that are in similar industries* as those discussed during calls."

This evidently common deficiency smacks of the kind of "shadow trading" the Enforcement staff targeted in *Panuwat* – and marks the first time the SEC has explicitly stated a requirement to address "shadow trading" through advisory firms' compliance apparatus. The alert is characteristically light on specific guidance, but nevertheless signals that staff throughout the agency are focusing on "shadow trading." The Risk Alert makes clear that firms should consider whether they need to do more to address the risk that supervised persons are executing trades in the securities of publicly traded companies "that are in similar industries" to companies about which they possess potential MNPI.

A Focus on Private Equity

Unsurprisingly, perhaps, the staff is likely to focus on advisers to private funds. In its 2022 Examination Priorities, EXAMS counted private funds first among its "Significant Focus Areas," given "the significance of examination findings over the past several years, and the size, complexity, and significant growth of this market." *See Division of Examinations 2022 Examination Priorities* (January 2022). The recent EXAMS Risk Alert confirms that the division views oversight of advisers to private funds as a programmatic imperative.

In 2020, the Commission brought an enforcement action against Ares Management, which creates a path for the SEC to craft an enforcement action against a firm that fails to address risks of "shadow trading" *even if* the SEC cannot prove any illicit trading. In *Ares*, the SEC alleged that the investment firm failed to implement and enforce adequate policies and procedures to prevent the misuse of "potential" MNPI. *See Private Equity Firm Ares Management LLC Charged with Compliance Failures*, SEC Press Release 2020-123 (May 26, 2020). The SEC's charges centered on Ares's failure to implement adequate policies and procedures to ensure that the company had not obtained MNPI about a portfolio company for which

one of its traders served on the board of directors. Notably, the SEC faulted Ares's compliance personnel for allowing supervised employees to "self-evaluate" whether potential MNPI was "material," suggesting that Ares's compliance personnel should have independently probed whether the "potential MNPI" was in fact MNPI. The SEC charged the firm for these purported compliance failures, though it did *not* allege that the firm actually misused the potential MNPI at issue.

Ares marked the first time the SEC faulted an adviser for its failures with respect to "potential MNPI" – and effectively ramped up the compliance burden to continuously assess potential MNPI. In this light, the SEC's increased focus on "shadow trading" is particularly expansive.

Compliance Response

Understandably, the SEC's interest in "shadow trading" has captured the attention of registered investment advisers who are grappling with the compliance implications of this new theory. The SEC has effectively put advisory firms on notice that they should enhance compliance policies and procedures to police potential "shadow trading," but many advisers feel they have been left in the dark about the SEC's expectations, including whether they should design and implement appropriate new policies and procedures – and, if necessary, what those new policies and procedures should look like.

Given the lack of certainty about how far the SEC is willing to test its "shadow trading" theory outside of *Panuwat*, firms' response to these developments will depend in large part on individual risk appetites. Although we can only speculate on how the SEC's "shadow trading" theory might play out in contexts distinct from *Panuwat*, firms considering a proactive response to *Panuwat* would be well advised to scrutinize their compliance policies and procedures in three broad areas:

1. **Compliance Policy Language.** In *Panuwat*, the SEC relied heavily on the specific language of the MNPI policy at issue – and the Court in *Panuwat* endorsed that reliance. Compliance professionals should review their MNPI policies to ensure the wording cannot be interpreted more broadly than is intended, and that the policy is not vague about its obligations. Compliance professionals should similarly review the policies to ensure they aren't creating any additional monitoring or enforcement obligations that similarly are unintended. Compliance professionals in industry sectors where stock prices tend to move together are likely to face heightened scrutiny and should think critically about how the policy language could be mis-interpreted.
2. **Non-Disclosure Agreements.** Relatedly, given that the duty in *Panuwat* flowed entirely from the plain language of the MNPI policy at issue, compliance professionals considering whether a trader has received MNPI should scrutinize whether other contractual agreements – such as any NDAs governing the traders' receipt of the potential MNPI – create duties not to trade that are independent of those in the firms' compliance policies.
3. **Day-to-Day Monitoring of Potential MNPI.** Although the ultimate viability of the SEC's theories in *Panuwat* remains to be seen, compliance professionals who are approached by a trader with potential MNPI should consider whether there are new, post-*Panuwat* questions they should be asking that trader. Especially given the emphasis in *Ares* on compliance professionals' need to probe whether the potential MNPI at issue is in fact material, compliance professionals would do well to both consider some of the specific factors at play in *Panuwat* and potentially document their firm's consideration of same.

The reach and implications of the SEC's approach in *Panuwat* remain uncertain, especially given the lack of guidance at the motion to dismiss phase from the Court in *Panuwat*. The extent to which the SEC's focus on "shadow trading" will require firms to reconsider their compliance policies remains to be seen. But firms that are concerned about *Panuwat* need neither sit on their hands nor completely revise their compliance policies. The steps outlined above should provide adequate safeguards. In many cases, firms will simply continue to following existing practices when a supervised person receives potential MNPI, but expand their analysis to consider whether the MNPI covers economically-linked companies or industries.

Frequently Asked Questions on "Shadow Trading"

In conversations with clients and industry contacts, we frequently field questions about the potential reach of the SEC's "shadow trading" theory, and the appropriate compliance response. Following are our responses to several frequently asked questions. (These responses, of course, are not legal advice. Firms may wish to pursue different paths depending on a number of firm-specific factors.)

Q: We are concerned about how the SEC's "shadow trading" theory of insider trading may impact our compliance obligations. What is the first thing we should do?

A: Begin by revisiting your firm's policies and procedures. How do they define "material nonpublic information," and what do they instruct employees to do if/when they receive it? Consider whether policies might be enhanced to encourage traders, analysts, and the like to report the receipt of potential MNPI to

appropriate members of the compliance or legal teams.

Q: If a trader/analyst comes to us with a question about her/his receipt of potential MNPI, does this raise *Panuwat* issues?

A: It depends. The compliance or legal team will need to ask some questions: How did the trader/analyst receive the information? And from whom? Is there a formal or informal expectation that the trader/analyst will not use the information for certain purposes? Critically, does the trader/analyst plan to use the MNPI for a trade in a similar company or industry?

Q: If the trader/analyst is considering a trade/strategy in a similar company or industry, what should I do?

A: First, ask if there's an NDA (or similar agreement) that purports to restrict the use of the MNPI. If so, what limitations apply (*e.g.*, "only for purposes of fulfilling the contract / further the relationship")?

Second, if you are comfortable that there is not an agreement (*e.g.*, a provision in an NDA) that restricts trading in a similar industry, you might still consider a few additional factors before clearing the trade. For example, you might consider whether there are independent reasons for the investment decision/strategy and how similar the industries or companies are (*e.g.*, ask questions designed to ascertain the size of the industry/segment, how specific the information is to a particular company, or how broadly applicable the information may be). For example, information about a potential merger or acquisition in a tight industry (the situation in *Panuwat*) may require different treatment than information about supply chain issues in a massive global manufacturing industry.

Q: Should we prophylactically place names on the restricted list?

A: There is no simple answer to this question, but over-designation creates its own set of issues. The decision to place names on the firm's restricted list requires an analysis of all the relevant facts. You should consider the source of the information, restrictions on use, plans (or no plans) to use the information to trade, and whether the firm/fund already has positions in economically-linked companies, among other factors. The decision to wall-off supervised persons, or place names on a restricted list, should be largely the same analysis you have been conducting all along; now, you are simply considering additional factors that might suggest a prophylactic response is appropriate.

Q: If we determine that is safe to trade, what next?

A: Document the vetting process in the usual way (the same log/software you use to record MNPI questions in the ordinary course). Consider whether to note that compliance/legal personnel considered the size of the industry, broad applicability of the information, or other relevant factors in clearing the trade.

Q: If we determine that the trader/analyst should not trade in a similar entity, what should we do?

A: Again, you should document the process in the usual way. You will also need to determine what restrictions may be appropriate. This should be similar to the usual analysis: Do you need to place similar entities on a restricted list? Do you need to temporarily prohibit trading in an entire industry/segment? Can you safely wall off one or more employees that are aware of the potential MNPI?

Q: What else should we be doing?

A: This is an excellent time to conduct remedial training sessions or exercises, to make sure your team is attuned to "shadow trading" issues and the circumstances that should cause them to call compliance.

NOTED WITH INTEREST

Supreme Court Significantly Curtails Applicability of Section 1782 to International Arbitration

In 1964, the U.S. Congress amended 28 U.S.C.§ 1782(a) to permit district courts to order the production of certain evidence "for use in a foreign or international tribunal." Although Congress unquestionably intended in 1964 to broaden the applicability of the statute to include administrative and quasi-judicial proceedings beyond "judicial proceeding[s] . . . in any court in a foreign country," courts have disagreed as to whether Congress intended the phrase "foreign or international tribunal" to include international arbitrations.

In the recent consolidated cases of *ZF Automotive US, Inc. v. Luxshare, Ltd.* and *AlixPartners, LLP* v. *Fund for Protection of Investors' Rights in Foreign States*, the U.S. Supreme Court addressed whether the following two arbitral bodies constituted "foreign or international tribunal[s]": (i) an arbitration panel organized in accordance with a German-based private dispute resolution organization; and (ii) an ad hoc arbitration panel organized in accordance with the Arbitration Rules of the United Nations Commission of International Trade Law ("UNCITRAL") that was selected pursuant to a bilateral investment treaty. In both cases, the courts below held that these arbitral bodies were "foreign or international tribunal[s]" under § 1782. The Supreme Court, however, found they were not on the basis that a "foreign or international tribunal" under § 1782 must be a governmental or intergovernmental adjudicative body, and neither arbitral body was "imbued with governmental authority."

1. Meaning of "Tribunal" in 28 U.S.C. § 1782

The first issue addressed by the Supreme Court was "whether the phrase 'foreign or international tribunal' in § 1782

includes private adjudicative bodies or only governmental or intergovernmental bodies." In addressing this question, the Court began with a narrow focus on the word "tribunal." The Court, looking at dictionary definitions, acknowledged that the term can be used synonymously with "court," but, in light of Congress's amendments to § 1782, "tribunal" should be understood in the broader sense as referring to "any adjudicatory body." Notably, the Court recognized that this broad meaning of tribunal does not itself exclude private adjudicatory bodies, but the Court explained that its analysis did not end there. Rather, the Court explained that the phrase "foreign or international" modified the meaning of "tribunal." Accordingly, the Court held that "tribunal" as used in § 1782 means "an adjudicative body that exercises governmental authority."

The Court supported its holding that a "tribunal" under § 1782 must exercise governmental authority by looking to the history of § 1782 and comparing the statute of the Federal Arbitration Act ("FAA"). In 1964, Congress amended § 1782 by replacing the phrase "judicial proceedings" with "proceeding in a foreign or international tribunals." The Court explained that its decision to limit "tribunal" to bodies exercising governmental authority was consistent with Congress' amendment, which it read to signal an expansion of the types of *public* bodies covered by the statute. This made sense, according to the Court, because the "animating purpose of § 1782 is comity: Permitting federal courts to assist foreign and international governmental bodies promotes respect for foreign governments and encourages reciprocal assistance." Defining tribunal to include private arbitral bodies would not further this core purpose of § 1782 and would result in "significant tension" with the FAA, which, in the context of domestic arbitration, forecloses pre-arbitration discovery and only permits the arbitration panel to request discovery.

2. *When Do International Arbitral Tribunals Qualify as "Tribunals"?*

Having held that § 1782 requires a foreign or international tribunal to be governmental or intergovernmental, the Court next considered whether the two arbitral bodies at issue exercised governmental authority. The Court held that neither of the arbitral bodies at issue qualified as tribunals, with the status of the ad hoc arbitration panel presenting a "harder question" than the German private arbitration panel. The Court's rationale for its conclusion, particularly with respect to the ad hoc arbitration, provides future § 1782 applicants with guidance as to whether an arbitral body may qualify as a tribunal under § 1782.

In assessing the ad hoc arbitration panel's potential status as a § 1782 tribunal, the Court framed the "relevant question" as "whether the nations intended that the ad hoc panel exercise governmental authority." Concluding that they did not, the Court, recognizing that "governmental and intergovernmental bodies may take many forms," left the door open to the "possibility that sovereigns might imbue an ad hoc arbitration panel with official authority." In doing so, the Court's decision recognized several factors (or as the Court put it, "indicia," "indications," "features," or "other evidence") that are relevant to the issue of whether the relevant sovereign(s) intended for an arbitral body to exercise governmental authority:

1. *Whether the arbitral body is a pre-existing body or formed for the purpose of adjudicating disputes*. The Court stated that the ad hoc arbitration panel was formed for the purpose of adjudicating investor-state disputes and as such was not a pre-existing tribunal.
2. *Whether the arbitral body is created by an international treaty itself or the sovereigns thereto are involved in its formation*. The Court stated that the treaty did not create the ad hoc arbitration panel but rather merely references the set of rules that govern the panel's formation and procedures.
3. *Whether the arbitral body is affiliated with a sovereign.* The Court stated that the ad hoc arbitration panel "function[ed] independently" of the sovereigns, consisted of individuals chosen by the parties, and lacked an "official affiliation" with the sovereigns or any other governmental or intergovernmental entity.
4. *Whether the arbitral body receives government funding.* The Court stated that the ad hoc arbitration panel did not receive any government funding.
5. *Whether the arbitral proceedings are public*. The Court noted that the ad hoc arbitration panel's proceedings maintained confidentiality.
6. *Whether the arbitral award is public.* The Court noted that an award issued by the ad hoc arbitration panel could only be made public with the consent of both parties.
7. *Whether the tribunal's authority exists because sovereigns "clothed the panel with governmental authority."* The Court stated that the ad hoc arbitration panel had authority because the parties consented to the arbitration, not because of any authority conferred.

Although the Court's opinion mentions the aforementioned considerations for determining whether an arbitral body exercises governmental authority, the Court did not strive to rank these considerations. Nor did the Court suggest that these factors are exhaustive or mandatory. Thus, we anticipate that, in the wake of the Supreme Court's opinion, some § 1782 applicants will continue to seek discovery for use in a foreign or international arbitration proceeding where the arbitral body possesses one or more of the aforementioned characteristics. The saga between § 1782 and arbitration continues, albeit in a more limited fashion.

Antitrust & Competition Update

Labor Market Restrictions Remain in DOJ Crosshairs

The US DOJ Antitrust Division has recently reaffirmed its long-stated intention to proceed criminally against naked wage-fixing and no-poaching agreements. That remains, despite the recent acquittals in its first two jury trials of these types of criminal charges.

According to the US antitrust agencies, competitors are likely violating the antitrust laws if they agree to fix wages to employees ("wage-fixing"), or to not solicit or hire each other's employees ("no-poaching"). DOJ & FTC, *Antitrust Guidance for Human Resource Professionals* 3 (Oct. 2016). The agencies' position is that naked wage-fixing or no-poaching agreements are *per se* illegal, that is, illegal without consideration of any procompetitive efficiencies. *Id.* at 3. Agreements among competitors are "naked" if they are separate from or not reasonably necessary to a larger legitimate collaboration among them. *Id.* In contrast, in the agencies' view, legitimate joint ventures are not considered *per se* illegal under the antitrust laws. *Id.*

Over the years, the DOJ has shifted to a more aggressive policy toward these types of naked agreements. In October 2016, the DOJ announced the shift: "Going forward, the DOJ intends to proceed criminally against naked wage-fixing or no-poaching agreements." *Id.* at 4. The Biden administration has subsequently supported this policy. During the campaign, the Biden Plan sought to "[e]liminate non-compete clauses and no-poaching agreements that hinder the ability of employees to seek higher wages, better benefits, and working conditions by changing employers." The Biden Plan for Strengthening Worker Organizing, Collective Bargaining, and Unions. In July 2021, President Biden issued an Executive Order seeking, among other things, "[t]o better protect workers from wage collusion" and "[t]o address agreements that may unduly limit workers' ability to change jobs". Executive Order on Promoting Competition in the American Economy (July 9, 2021).

Pursuant to this policy shift since 2016, the DOJ obtained its first wage-fixing criminal indictment, which was of the former owner of a physical therapist staffing company, in December 2020. *U.S. v. Jindal*, Case No. 4:20-cr-00358 (E.D. Tex.). The DOJ obtained its first no-poaching criminal indictment, which was of a healthcare company and a related entity, in January 2021. *U.S. v. Surgical Care Affiliates, LLC*, Case No. 3:21-cr-00011 (N.D. Tex.). The DOJ obtained a related no-poaching criminal indictment of another healthcare company and its former CEO in July 2021. *U.S. v. DaVita Inc.*, Case No. 1:21-cr-00229 (D. Colo.).

In all three cases, the defendants moved to dismiss the indictments, arguing that there is no due process or fair notice because there is no judicial precedent holding that wage-fixing or no-poaching agreements are *per se* illegal and therefore subject to criminal prosecution. In *Surgical Care Affiliates* and *DaVita*, the US Chamber of Commerce filed an amicus brief arguing these grounds and that the DOJ's policy shift violates separation of powers by usurping the power of the judiciary and legislature to decide what types of agreements are *per se* illegal and therefore subject to criminal prosecution.

In two of these cases, the courts denied the motions on these grounds. In *Jindal*, on November 29, 2021, the court concluded that the wage-fixing agreement alleged in that case, if proven, would amount to price-fixing among competitors, which is an existing category of *per se* illegal agreement recognized in the case law. In *DaVita*, on January 28, 2022, the court concluded that the no-poaching agreement alleged in that case, if proven, would amount to a means of market allocation among competitors, which is another existing category of *per se* illegal agreement. In *Surgical Care Affiliates,* the motion to dismiss is still pending.

While the courts denied the motions, a Texas federal jury found the defendants not guilty of the wage-fixing charges in *Jindal* on April 14, 2022, and the next day, a Colorado federal jury found the defendants not guilty of the no-poaching charges in *DaVita*. Only Mr. Jindal was found guilty, on an obstruction charge that did not require proof of an antitrust violation.

Despite the acquittals, the DOJ has confirmed its commitment to pursuing these criminal antitrust cases. The DOJ has publicly stated that it is actively pursuing nearly 20 criminal antitrust cases, including *Surgical Care Affiliates*; a wage-fixing and no-poaching case against a health care staffing company and its former regional manager, *U.S. v. Hee*, Case No. 2:21-cr-00098 (D. Nev.); a wage-fixing and no-poaching case against four owners or operators of home health care agencies, *U.S. v. Manahe*, Case No. 2:22-cr-00013 (D. Me.); and a no-poaching case against a former manager of a major aerospace engineering company and five current and former executives of outsource engineering suppliers, *U.S. v. Patel*, Case No. 3:21-cr-00220 (D. Conn.). Several of these indictments were followed by private class action litigation. In order to pursue these and other matters, the Biden administration has sought $88 million in new funding for the DOJ Antitrust Division in 2023.

After the verdicts, Jonathan Kanter, Assistant Attorney General of the DOJ Antitrust Division, stated the need for the DOJ to strengthen its resolve in bringing these kinds of cases, if righteous, even if difficult, valuing court decisions finding these cases legally sound, and public demand for more of these cases, over jury verdicts

in individual cases. Other DOJ officials have expressed similar sentiments. Companies and individuals engaged in these kinds of agreements should anticipate the risk of further criminal prosecution by the DOJ and class actions by private plaintiffs.

Artificial Intelligence Update

NIST Proposes Comprehensive Risk Management Framework for AI

As advances in artificial intelligence ("AI") have led to widespread adoption of AI-based applications, the potential that AI systems could produce unwanted and potentially harmful results has attracted increased scrutiny from policymakers. Among other concerns, policymakers seek to ensure that AI systems avoid harmful bias and are accurate, explainable, and protective of privacy. In the past, these issues have been addressed in the U.S. through a patchwork of regulatory and state legislative actions, generally targeted at specific applications or issues.

In 2019, the Trump Administration issued the Executive Order on Maintaining American Leadership in AI, which, among other things, directed the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") to create a comprehensive "plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies." E.O. 13859 (Feb 11, 2019). In 2020, Congress directed NIST to develop an AI Risk Management Framework ("AI RMF"). *See* Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2021, H. Rept. 116-455, 116th Cong. (Jul. 16, 2020). On March 17, 2022, the NIST released the first draft of its Artificial Intelligence Risk Management Framework (the "AI RMF"). *See* https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf.

A. Draft AI RMF

The draft AI RMF uses a three-class taxonomy to classify AI characteristics by which AI can be assessed as trustworthy or risky: 1) technical characteristics, (2) socio-technical characteristics, and (3) guiding principles. Technical characteristics refer to risks in the design of the AI system, and include accuracy, reliability, robustness, and resilience/security. Socio-technical characteristics refer to the human and systemic institutional and societal biases that impact the way AI systems are used and perceived in society, including explainability, interpretability, privacy, safety, and managing bias. Guiding principles refer to broader societal norms and values to which AI systems should adhere, including fairness, accountability, and transparency.

Referencing this framework, the draft AI RMF sets out a list of actions that organizations can take to identify and mitigate the relevant risks for particular AI systems. The draft AI RMF organizes these actions into four functions: Map, Measure, Manage, and Govern, which should be iteratively performed.

Following a public workshop on the draft AI RMF in March 2022, the NIST and has released the first round of public comments, which includes input from a wide variety of stakeholders from industry, government, and higher education, including Google, Kaiser Permanente, the Bureau of Labor Statistics, the American Property Casualty Insurance Association, the Recording Industry Association of America, the U.S. Chamber of Commerce, and U.C. Berkeley. *See* https://www.nist.gov/itl/ai-risk-management-framework. The NIST plans to conduct another workshop on October 19-21, 2022, and release the final version in late 2022 or early 2023. *Id.*; https://www.nist.gov/itl/ai-risk-management-framework/ai-risk-management-framework-workshops-events.

B. Current Legislation and Regulation of AI

AI regulations to date have been directed to only a subset of the risks identified by the draft AI RMF. Currently no federal legislation governs AI systems in the U.S., but federal oversight has come from regulatory agencies, including the Federal Trade Commission, the Department of Housing and Urban Development, and the Equal Employment Opportunity Commission. The scope of their regulation is necessarily limited – for example, the FTC's rulemaking is limited to addressing discriminatory and fraudulent business practices and the EEOC focuses on the use of AI in hiring and workplace applications.

At least five states (Alabama, Colorado, Illinois, Mississippi, and Utah) have passed legislation related to AI, and legislation is pending in over a dozen more. *See* https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx. However, so far, state legislation has also been limited in scope. For example, Illinois has focused on regulating bias in AI systems used for employment decisions, and Alabama's bill simply created an advisory council on AI.

Even the proposed European Union AI Act, which is the most comprehensive AI legislation proposed to date, does not explicitly address certain technical and socio-technical risks such as accuracy, explainability, and interpretability, and has been criticized for its lack of a process to reclassify AI systems based on future developments. *See, e.g.,* EDRi et al., *An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement*, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf. The AI RMF's efforts to address the full spectrum of AI risks may enable more

comprehensive future legislation or regulation.

C. Potential Impact of the AI RMF

Despite its voluntary nature, the AI RMF itself may effectively impose legal obligations on developers and users of AI systems by informing the common law standard of care. As disputes arise regarding harms caused by AI systems, courts may look to the AI RMF to determine whether there are additional actions that should have been taken to prevent those harms. There is some precedent for using voluntary NIST frameworks as a standard of care. In 2014, the NIST released a voluntary cybersecurity framework. Commentators recognized that it could be adopted as a standard of care. *See, e.g.,* Scott J. Shackelford *et al., Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. Int'l L.J. 305 (2015). And courts have recognized its value in informing the standard of care. For example, expert testimony in a voting rights case invoked the NIST cybersecurity framework in opining about the appropriate standard of care. *See Curling v. Raffensperger*, 397 F. Supp. 3d 1334, 1376 n.59 (N.D. Ga. 2019). And compliance with the cybersecurity framework was a condition of the settlement of class action litigation over Yahoo's data security breach in 2020. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2020 WL 4212811, at *33 (N.D. Cal. July 22, 2020). The AI RMF is likely to be used similarly to establish a standard of care in future litigation over AI systems.

For now, the AI RMF can help organizations address the emerging patchwork of legal requirements applying to AI systems, and prepare for future comprehensive regulation. The NIST privacy framework, released in 2020, has served a similar role. At the time the privacy framework was released, the E.U. General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") were the only significant data privacy laws in effect. Since then, over 60% of states have considered or passed new privacy regulations. The privacy framework has helped organizations anticipate and keep up with the wave of privacy regulations. As AI regulation moves forward on a similar trajectory, the AI RMF will likely prove a useful tool for organizations to keep up with the rapidly evolving legal landscape.

Regulating Deepfakes: New Consequences for Platforms and Producers

In March 2022, a widely circulated video seemed to show Ukrainian President Volodymyr Zelenskyy calling upon Ukrainians to lay down their weapons and surrender to Russia. The video was fake, and debunked by President Zelenskyy himself, but its popularity illustrates the ability of deepfakes to influence the public and potentially affect the political landscape.

Two weeks later, a deepfake video went viral that seemed to show American actor Tom Cruise at the American Film Institute awards show jumping over the head of a presenter, garnering over ten million views and bringing the conversation of created fake realities back into public debate.

Deepfakes are realistic, but fake, videos made using machine learning and artificial intelligence software. The quality of deepfake videos is consistently increasing, making them harder to detect as false. Since 2019, a handful of jurisdictions around the world have introduced legislation to address deepfakes, taking divergent approaches to address either harm occurring at the societal or individual level by targeting the producers of deepfakes or the distributors that host them. With respect to harm on a societal level, regulations and legislation criminalizing or prohibiting the dissemination of deepfakes seek to target deepfake distributors and producers. On the individual level, persons whose likeness has been used may have a cause of action against the producer responsible for making the deepfake; or against the platform that hosts or disseminates it.

Addressing Societal Harm

Deepfakes fall under the prohibited practices of the EU's Code of Practice on Disinformation ("Code"). To address societal harms of false information, the European Commission unveiled on June 16, 2022 a strengthened Code with the goal of developing "very significant commitments to reduce the impact of disinformation online and much more robust tools to measure how these are implemented across the EU in all countries and in all its languages." European Commission Press Release (Jun. 16, 2022). The European Commission Vice-President for Values and Transparency, Věra Jourová, cited the weaponization of information by Russia and attacks on democracy more broadly as considerations behind the strengthened Code, which provides a meaningful measure to address disinformation and achieve a cohesive set of commitments and understanding for platforms. With the introduction of the new Code, large technology companies—including Google, Meta (parent company of Facebook, Instagram and WhatsApp), Twitter, and TikTok—must take measures to counter deepfakes and false accounts on their platforms—or face significant fines of up to 6% of their global turnover.

The Code, initially introduced in 2018 as a voluntary self-regulatory instrument by industry players, will now have the backing of the Digital Services Act ("DSA"), a comprehensive set of rules that the European Commission has been working towards finalizing since 2018 to protect consumers online, establish a framework of transparency and accountability for online platforms and foster

competitiveness. The DSA seeks to impose rules on how platforms moderate content, advertise and use algorithms. The Code's signatories will be subject to the DSA's audit requirements and dissuasive sanctions if they fail to comply with their obligations.

Platforms that reach more than 10% of the EU population, meaning they have at least 45 million users in the EU, are designated under the DSA as "Very Large Online Platforms" and have a specific set of obligations due to the "systemic risks the platform poses [that] have a disproportionately negative impact in the Union." The Very Large Online Platforms that signed onto the Code have committed "to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviors, actors and practices not permitted on their services," including malicious deep fakes, creation and use of fake accounts, account takeovers and bot-driven amplification, non-transparent paid messages or promotion by influencers, hack-and-leak operations and under conduct aimed at artificially amplifying the reach or perceived public support for disinformation. Code, Commitment 14. The Code's 34 signatories, which include Google, Meta, Microsoft, TikTok, Twitter, Vimeo, World Federation of Advertisers (WFA), Interactive Advertising Bureau (IAB Europe), and European Association of Communication Agencies (EACA), have six months to implement the commitments and measures they agreed to and must report to the Commission by early 2023 their implementation.

The approach of addressing deepfakes by targeting platforms responsible for distributing and hosting them was previously implemented in China, which in 2019 made it a criminal offense to publish deepfake videos created with artificial intelligence or virtual reality, beginning January 1, 2020. The Cyberspace Administration of China, in implementing regulations requiring all deepfakes to be prominently labeled and prohibiting deepfakes used as fake news, explained its reasoning that deepfakes create risks of "endangering national security, undermining social stability, disrupting social order, and infringing on the legitimate rights and interests of others, causing political security risks, national security, and public security risks, and adversely affecting social stability." Cyberspace Administration of China, Briefing (Nov. 29, 2019).

Certain U.S. jurisdictions target the producer of a deepfake under certain circumstances. For example, in the U.S. state of Texas, it is a crime to make and publish or distribute a deepfake video with the intent of injuring a political candidate or influencing the result of an election. Such laws may end up being hard to enforce given the difficulty in finding the producer of the deepfake videos, and ultimately even with enforcement the video may remain online without additional measures to require its removal from distribution platforms. Once a violation is established, the platform can be notified to remove the content voluntarily or in accordance with industry self-regulatory commitments.

Addressing Individual Harm

The law has moved more slowly than technology in addressing harm to individuals caused by deepfakes. Aside from a few jurisdictions, laws have not been introduced to specifically address deepfakes or provide causes of action to individuals whose image or likeness has been used in a deepfake.

Within the U.S., for example, laws that have been introduced are narrowly tailored to address two primary concerns for how deepfakes could be used: (i) to interfere with elections; or (ii) to develop sexually explicit content. Individuals harmed by deepfake technology have, with varying degrees of success, sought redress in courts against producers and distributors using existing causes of action that were not developed specifically for deepfakes. For example, subjects of deepfakes may assert claims that their image, expression or voice are copyrighted material and their use violates copyright laws. These claims face difficulties overcoming broad exceptions to copyright infringement, for example with the "fair use" doctrine in the U.S. that allows for the unlicensed use of material that would otherwise be prohibited under copyright laws if, for example, the borrowed content were sufficiently transformed. In practice, the copyright holder may have more success focusing its efforts towards the platform rather than the producer, *i.e.* by posting a takedown notice or requesting that the platform voluntarily remove or flag the deepfake. Similarly, if the deepfake is used in commercial advertising, an action may lie under the Lanham Act.

Targets of deepfakes may also have a claim for defamation, *i.e.* due to injury to their reputation caused by the deep fake, or under various torts such as the tort of false light, invasion of privacy or the right of publicity, depending on the jurisdiction.

As deepfakes evolve, so too do laws, regulations, and political will to address the issue, so it remains to be seen how this area will develop. One thing seems certain: the days of unregulated platform content are over.

Complete Defense Verdict for AIG in Major Insurance Fraud Dispute

The firm recently obtained a hard-fought and decisive jury verdict for AIG Specialty Insurance Company and Lexington Insurance Company, providing them with a complete defense to coverage of a $236 million Medicaid Fraud settlement. The Quinn Emanuel team not only represented AIG Specialty Insurance Company and Lexington Insurance Company, but also served as lead trial counsel for all insurers that went to trial. The plaintiff, Conduent State Healthcare LLC ("Conduent"), paid $236 million (a record in Texas!) to settle a Medicaid Fraud claim brought by the Texas Attorney General's Office, and Conduent thought that it could game the settlement process to force its tower of insurers to indemnify Conduent for the payment. A Delaware jury said no.

For several years leading up to the $236 million settlement, the Texas Attorney General investigated and pursued a Medicaid Fraud claim against Conduent. During this time, the Texas Attorney General informed Conduent that it was seeking over $2 billion in civil fines and penalties resulting from Conduent's alleged Medicaid Fraud. Throughout the Medicaid Fraud case, Conduent repeatedly attempted to bring additional parties into the suit to allocate its liability to such parties and reduce its overall liability. However, in mid-2018, the Texas Supreme Court held that Conduent was forbidden from doing so. The Court specifically found that the Medicaid Fraud claim could not be allocated among multiple parties and that Conduent had to defend its suit alone.

In the wake of this loss at the Texas Supreme Court, Conduent engaged with the Texas Attorney General's Office to discuss a settlement of the Medicaid Fraud claim. During these discussions, Conduent adamantly pressed the Texas Attorney General to add a breach of contract claim and a negligence claim to Texas's case against Conduent. The Texas Attorney General repeatedly refused this request, but after receiving an ultimatum from Conduent deep in the settlement negotiations, Texas relented and amended its petition to include the additional claims. On the same day that Texas added the new claims, the parties executed a settlement agreement that allocated all of the proceeds of the settlement to the brand new claims for breach of contract and negligence, and none of the settlement proceeds to the claim for Medicaid Fraud. This was no coincidence. Conduent and its insurers had discussed the Medicaid Fraud case on several occasions, and Conduent knew that the insurers would not cover any amount allocated to the claim for Medicaid Fraud based on several exclusions in the insurance policies. So, in an attempt to secure coverage, Conduent pressured the state to amend and then allocated all of the settlement proceeds away from the Medicaid Fraud claim.

Needless to say, the insurers were not informed of Conduent's campaign to pressure Texas to amend its petition. Indeed, the only communications they received from Conduent created the misleading impression that the Texas Attorney General made the decision, of its own volition, to add these new claims for the purpose of prosecuting them to completion. After being left in the dark, the insurers were handed a finalized settlement agreement and an amended petition and were asked to provide coverage. The insurers rightly refused. It was only during the course of litigation—through discovery—that the insurers finally learned the details of Conduent's scheme to manufacture coverage. And the details of this scheme were laid bare before the jury in Delaware.

After a six-day trial, the Delaware jury took only two hours to find in favor of the insurers on several grounds. The jury found that Conduent had committed insurance fraud, breached its duty to cooperate, and failed to settle the Texas case in good faith, findings that gave the insurers a complete coverage defense.

Rare EU Antitrust Victory Before the EU General Court for Qualcomm

Following an utterly inadequate "investigation" sparked, as it would transpire much later, by an informal complaint made by a third-party in summer 2014, the European Commission ("Commission") adopted in January 2018 a decision finding that Qualcomm had abused a dominant position by entering into an agreement with Apple providing for payments conditioned upon Apple buying LTE chipsets exclusively from Qualcomm. The decision imposed on Qualcomm a fine of EUR 997 million (c. USD 1 billion) – one of the highest fines ever imposed by the Commission for a violation of the EU's antitrust laws.

In April 2018, Qualcomm filed with the EU General Court an application seeking the annulment of the Commission's decision. There followed several further rounds of written pleadings, including the submission by Qualcomm in July 2019 of dozens of documents obtained from Apple as a result of Section 1782 discovery proceedings brought by Qualcomm in the U.S.. Those documents proved to be crucial: they contained material that not only revealed grave breaches of Qualcomm's rights of defence committed during the investigative phase but also impugned the theory of harm underpinning the Commission's final decision attaching antitrust liability. The case was argued during a three-day oral hearing held in May 2021 before the EU General Court.

In a landmark judgment handed down on 15 June

2022, the Court annulled in its entirety the Commission's decision. The ruling is an unprecedented and emphatic win for Qualcomm that vindicates the creative, tenacious, and, when required, aggressive, legal strategy adopted in this case from its inception in summer 2014.

More specifically, the General Court annulled in full the Commission's decision on various procedural grounds (multiple failures to observe due process during the investigation) as well as on substantive grounds (manifest errors in assessing the actual and potential anticompetitive effects of Qualcomm's conduct).

Regarding procedure:

- The Court found that the Commission had failed to keep proper notes of meetings with third parties or to provide them to Qualcomm at a time when they would have allowed Qualcomm to exercise its rights of defence. The Court described the notes belatedly provided to Qualcomm as "*meaningless*," accepted Qualcomm's argument that a number of them were actually drawn up or edited years after the relevant meetings took place, and condemned the Commission's overall "*lack of precision*" in compiling the investigation file; and
- The Court held that Qualcomm had not been given the opportunity to defend itself adequately in respect of important elements of the Commission's decision. Notably, between the statement of objections (in essence, the charge sheet) and the final decision, the Commission changed the theory of harm pursued and dropped its objections in relation to certain chipsets found to belong to a different relevant product market without affording Qualcomm the opportunity to submit new economic evidence and comment on the Commission's revised position.

Regarding substance:

- The Court reasoned that the Commission had failed to establish that the impugned conduct could produce the actual or potential anticompetitive effects alleged in the decision. The Commission had failed properly to apply the governing EU case law and, in particular, to take account of "*all the relevant factual circumstances*," e.g., the fact that, for much of the period concerned, Qualcomm's rivals were unable to offer chipsets capable of satisfying Apple's technical requirements; and
- The Court held that Commission's analysis of "actual effects," i.e., findings made in respect of the alleged foreclosure of rival chipset suppliers from certain 2014 and 2015 cellular iPads, were "*vitiated by a lack of consistency in the evidence relied on in support of its findings*." The Court reiterated that the analysis of anticompetitive capability cannot be purely hypothetical, held that the Commission's assessment did not support the conclusion that the payments made by Qualcomm had reduced Apple's incentives to switch to a rival chipset supplier, and found that the Apple documents and submissions on which the decision relied did not support its findings regarding the alleged foreclosure.

Although the judgment may be appealed to the Court of Justice of the EU, it seems unlikely that it would be overturned. This is because the General Court went to great pains to examine and adjudicate on a large numbers of pleas each of which, on its own, would have justified annulling the Commission's decision.

Prevailing in abuse of dominance cases is extremely rare: the present case appears to mark the first time in 20 years the Court has quashed at first instance a Commission abuse of dominance decision. This is also a pioneering case, in that it constitutes the first time the EU Courts, which traditionally reject the use of "foreign" documents in cases before them, have accepted evidence obtained through Section 1782 proceedings.

Landmark Trial Victory in Delaware Chancery Court

The firm secured a landmark trial victory on June 16, 2022 when Vice Chancellor Lori W. Will of the Delaware Court of Chancery issued a 65-page post-trial opinion granting a declaratory judgment, permanent injunction, and other equitable relief for our client Warren Lichtenstein. Lichtenstein is the Executive Chairman of investment company Steel Partners Holdings L.P. ("Steel"), and previously also served as Executive Chairman of propulsion systems manufacturer Aerojet Rocketdyne Holdings, Inc. ("AJRD"). On February 7, 2022, Lichtenstein and three other AJRD directors filed a complaint against the Company's other four directors—including its CEO Eileen Drake—seeking to prevent the unauthorized use of corporate resources in an ongoing contest for control of the Company.

After AJRD's deadlocked board was unable to agree on a Company slate of director nominees for the upcoming shareholder election, Steel nominated its own slate (including all four eventual plaintiffs) and Drake nominated her own (including all four eventual defendants). When Steel nominated its slate, Drake issued an official Company press release and SEC filings disparaging Lichtenstein, and engaged Company counsel and advisors to oppose Steel's slate and promote her own. Quinn Emanuel sued to stop Drake from continuing to mobilize AJRD's resources against Lichtenstein without authorization, requesting a declaratory judgment and equitable relief and, in the meantime, a temporary restraining order.

Quinn Emanuel won both. The court quickly

granted the TRO, agreeing that a Delaware corporation's management cannot act for the Company without authorization from a majority of the Board and ordering AJRD to stay neutral in the proxy contest as long as the Board remained deadlocked. Then, following a three-day trial in May, the Court reaffirmed that principle of corporate neutrality—holding that "The Company, which is necessarily guided by the Board, could not (and cannot) take sides pending the outcome of the election" because "[t]o hold that one stockholder-nominated slate comprising half of the incumbent directors can advantage itself with access to the company's name, funds, and employees because it includes management would unfairly tip the scales in that slate's favor." The Court also agreed with our client that the defendants had violated that principle, issued a declaratory judgment for our client, permanently enjoined further violations by the defendants, and ordered them to issue corrective disclosures retracting the unauthorized press release and SEC filings.

Vice Chancellor Will's opinion was both a resounding win for a Quinn Emanuel client and a significant ruling on a novel question of Delaware law, reaffirming the principle that a corporation can act only through its board in the unusual situation in which evenly divided board factions face off in a proxy contest. Q

quinn emanuel
865 South Figueroa Street, 10th Floor, Los Angeles, California 90017

business litigation report
quinn emanuel urquhart & sullivan, llp

Published by Quinn Emanuel Urquhart & Sullivan, LLP as a service to clients and friends of the firm. It is written by the firm's attorneys. The Noted with Interest section is a digest of articles and other published material. If you would like a copy of anything summarized here, please contact Elizabeth Urquhart at +44 20 7653 2311.

- We are a business litigation firm of more than 900 lawyers — the largest in the world devoted solely to business litigation and arbitration.
- As of July 2022, we have tried over 2,500 cases, winning 86% of them.
- When we represent defendants, our trial experience gets us better settlements or defense verdicts.
- When representing plaintiffs, our lawyers have garnered over $70 billion in judgments and settlements.
- We have won seven 9-figure jury verdicts and four 10-figure jury verdicts.
- We have also obtained fifty-one 9-figure settlements and nineteen 10-figure settlements.

Prior results do not guarantee a similar outcome.

ATLANTA
AUSTIN
BOSTON
BRUSSELS
CHICAGO
DOHA
HAMBURG
HONG KONG
HOUSTON
LONDON
LOS ANGELES
MANNHEIM
MIAMI
MUNICH
NEUILLY-LA DEFENSE
NEW YORK
PARIS
PERTH
RIYADH
SALT LAKE CITY
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STUTTGART
SYDNEY
TOKYO
WASHINGTON, D.C.
ZURICH