January 2017

quinn emanuel

quinn emanuel urquhart & sullivan, llp | business litigation report

los angeles | new york | san francisco | silicon valley | chicago | washington, d.c. | houston | seattle
tokyo | london | mannheim | hamburg | munich | paris | moscow | hong kong | sydney | brussels | zurich | shanghai

China's 2016 Cybersecurity Law Will Change the Way Multinational Companies Do Business in China

China adopted its controversial Cybersecurity Law on November 7, 2016. The law, which will take effect on June 1, 2017, has broad implications for how multinational companies operate in China. The law addresses a number of issues, including requiring certain companies to pass national security reviews, store user and business data in mainland China, and to provide technical support to Chinese authorities.

Broad Applicability

The law imposes obligations on two tiers of businesses: network operators and critical information infrastructure operators. "Network operators" are defined as owners or providers of any "network," which in turn is defined as any system of computers or other terminals that collect, store, transmit, and process information. (Article 76.) Given the broad definition of a network—it likely includes most Internet platforms or any two connected computers—most businesses will come within the scope of this term. "Critical information infrastructure operators" are not precisely defined, but Article 31 suggests it includes any businesses operating in the communications, finance, water, power, or traffic sectors, as well as any other businesses using infrastructure that could harm China's security, economy, or citizens if it were to fail. The law imposes stricter obligations on businesses coming within the scope of this term.

Technology Reviews, Inspections, and Certifications

The law imposes several requirements on the security of certain network products and services. Article 23, for example, requires "key network equipment and network security products" to meet China's national standards and mandatory requirements. Also, before such equipment or products may be used in China, the equipment and products must either pass a safety inspection or be safety certified by a qualified agency. (Article 23.) The law states that the Chinese government will release a catalog of the types of network equipment and products subject to this requirement (*id.*), as well as the national standards and requirements that specific equipment

(continued on page 2)

INSIDE

Quinn Emanuel Hosts California EU Antitrust Enforcement Seminar

The firm was pleased to welcome in-house counsel to a series of seminars on recent developments in EU antitrust enforcement. The seminars were held in Silicon Valley, San Francisco, and Los Angeles. Partners Trevor Soames and Dr. Nadine Herrmann presented insiders' perspectives of key antitrust issues, including 2017 antitrust enforcement initiatives under Commissioner Vestager; BREXIT impact on antitrust enforcement and litigation in the EU27 and the UK; IPR, especially SEPs (FRAND, injunctive relief, royalty rate, SSPPU, FRAND obligations to license third parties); and Big Data. Trevor Soames is a leading European antitrust practitioner and managing partner of Quinn Emanuel's Brussels office. Dr. Nadine Herrmann is managing partner in Quinn Emanuel's Hamburg office and chair of the firm's EU and German Competition Law Practice.

Quinn Emanuel Elects Thirteen New Partners

See page 8

and products must satisfy (Article 15), at some time in the future.

This requirement effectively narrows the types of network equipment and products that companies may use to a limited group of pre-approved technology. Companies that make key network equipment or products are likely to face challenges in ensuring their products meet China's not-yet-released standards, and companies that use key network equipment and products will face similar challenges in obtaining approval for their use by a safety inspection or certification. The law does not specify the timeline for the certification process, which conceivably could take long enough to delay a product to market in China. Nor does the law specify how intrusively products will be "investigated," which conceivably could include examinations of a company's intellectual property and trade secrets.

Further obligations apply solely to critical information infrastructure operators, including a requirement that they undergo a "national security review" before purchasing any products or services that "may affect national security." (Article 35.) The law does not describe what such a national security review entails, nor does it specify the types of products or services that may affect national security. Questions also remain as to the intrusiveness of the national security reviews, such as whether they will require disclosure of intellectual property or trade secrets.

Data Localization in Mainland China

Critical information infrastructure operators are also subject to a data localization rule, which requires they store "personal information"—*e.g.*, name, birthdate, address, number—and "other important data" related to their Chinese operations on servers located within mainland China. (Article 37.) Although earlier drafts of the law referred to "citizens' personal information," the final version removed the reference to "citizens," thus suggesting that "personal information" includes information of both citizens and foreigners. The law does not define "other important data."

An operator may not send either category of information outside of China unless the operator can show it is "truly necessary" for business reasons and has passed the government's "security assessment." (Article 37.) The law does not define "truly necessary," nor does it specify the requirements to pass a "security assessment." Notably, while an earlier draft would have allowed operators to "send" and "store" such information abroad, the final law deleted the reference to "store." Thus, the law likely prohibits operators from storing any such information abroad, even if it was necessary and passed a security assessment.

Multinational companies, which often rely on cross-border data flows, will find this requirement particularly troubling. Even under a narrow interpretation, a multinational company likely would have to segregate all information about its Chinese customers and their dealings onto Chinese servers. In effect, multinational companies would be required to have two global data systems: one for China and one for the rest of the world.

Close Cooperation with the Chinese Government

The law also requires companies to work closely with Chinese government under various circumstances. Significantly, Article 28 requires network operators to "provide technical support and assistance" to government authorities when needed to preserve national security or investigate crimes. The law provides no further details concerning the type of technical support and assistance required.

Business and rights groups have questioned the true intent behind this requirement. Some commentators worry the Chinese government may invoke it to require technology companies to provide "backdoor" access to their products or other information concerning their technology, such as source code. Concerns also remain that network operators may become entangled in disputes concerning their users' online activities, particularly if Article 28 is invoked in conjunction with other provisions in the law. For example:

- Article 12 prohibits the use of any network to endanger national security, undermine national unity, or incite subversion, separatism, or the overthrow of the socialist system.
- Article 24 requires certain network operators—*e.g.*, Internet and phone providers, domain name registrars, publishing and blogging platforms, and instant messaging services—to obtain their users' real names before providing services.
- Article 21 requires network operators to monitor and log their networks' statuses and security incidents, as well as retain those logs for no less than six months.
- Articles 47 and 48 require network operators to "strengthen management of information published by users," and upon discovering that a user has transmitted "unlawful" information, the operator must stop the transmission and delete it from the public,

"save relevant records," and report the user to authorities.

- Article 58 allows the government to "take temporary measures regarding network communications," including "restricting" such communications, when necessary "to protect national security and social public order."

These articles, which reduce users' online anonymity and expand companies' obligations to monitor and report users, may pose significant public relations challenges for companies.

Looking Ahead

Although drafts of the law underwent several revisions and were subject to substantial debate, much of the final law still remains unclear. The law's few defined terms remain vague, and some of the most important terms are not defined at all. We expect Chinese authorities will issue further guidance in the coming months, which should provide more clarity regarding the scope of the law. In the meantime, we suggest that companies assess their exposure under the law, in particular whether they may qualify as "critical information infrastructure operators." Should a company potentially fall within that definition, internal risk assessment of its current compliance with this law and the work required to bring it into compliance would likely be warranted.

NOTED WITH INTEREST

Commercial Third Party Litigation Funders Exposed to Indemnity Costs in the UK

The UK Court of Appeal has held the funders of a losing claimant subject to a costs order on an indemnity basis as a result of the conduct of the claimant and its instructing solicitors. In *Excalibur Ventures LLC v Texas Keystone Inc & ors* (2016) EWCA Civ 1144, each funder was liable for the defendants' costs "to the extent of the funding" advanced. No distinction applied to funds earmarked solely for the provision of security for costs or to funders with no contractual relationship with the funded litigant.

In the underlying proceedings, an oil exploration firm founded by brothers Eric and Rex Wempum, Excalibur Ventures LLC (the "Claimant"), sought to recover its $1.6 billion interest in the Shaikan oilfield in Iraq from Gulf Keystone Petroleum Ltd and Texas Keystone Inc. (the "Defendants") by way of an order for specific performance of a Collaboration Agreement or damages. The asserted claims sounded in both contract and tort, and included fraud by concealment and by misrepresentation. Four groups of litigation funders including Psari Holdings Limited, Platinum Partners Credit Opportunities Master Fund LLP, Blackrobe Capital Partners LLC, and Platinum Partners Value Arbitrage Fund LP (the "Funders") advanced, between them, £32 million to meet the Claimant's legal costs including £17.5 million for the provision of security for costs.

At first instance, in the High Court, the claims failed on every point. Clarke LJ described the action as "replete with defects, illogicalities and inherent improbabilities." The Claimant was ordered to pay the Defendants legal costs on an indemnity basis—calculated as 85% of the Defendants' legal costs—as opposed to the lower rate, standard basis. Having determined that the £17.5 million previously paid into court would be insufficient on the indemnity basis, the Claimant was ordered, and failed, to advance an additional £5.6 million in funding. The Defendants then sought non-party costs orders against the Funders. The Funders either contested liability to meet the Defendants' legal costs altogether, accepted liability and contested the indemnity basis, or did not participate in the costs proceedings at all. Clarke LJ held the Funders jointly and severally liable to pay the Defendants' costs on the indemnity basis, subject to their only being liable in respect of costs incurred after the date of their first contribution.

On appeal by the Funders, the Court of Appeal considered (i) whether costs orders should be made against the Funders and if so, on what basis, (ii) whether funds made available for the purpose of enabling a litigant to furnish court-ordered security for costs should be distinguished, and (iii) whether funds who had no direct funding agreement with the Claimant but had provided funds on back-to-back terms through the direct funders were liable with their associated companies that directly provided funding.

The Funders contested liability for indemnity

costs because they had been guilty of no discreditable conduct. The appellate Court accepted that the Funders did nothing discreditable in the sense of being morally reprehensible or improper. Nonetheless, the argument suffered three fatal defects. First, it overlooked that under CPR 44, the conduct of the parties is only one factor to be taken into account when considering on what basis, if any, a costs order should be made. Secondly, the argument looked at the question from only one point of view, that of the Funder. It ignored the character of the action and its effect on the Defendants. Thirdly, it assumed that the Funder is responsible only for his own conduct. In fact, a litigant may find himself liable to pay indemnity costs on account of the conduct of those whom he chosen to engage such as lawyers or experts, or those he has chosen to enlist, such as witnesses.

The Association of Litigation Funders, as *amicus curiae*, suggested that, to avoid being fixed with the conduct of the funded party, funders would need to exercise greater control over the litigation process. Funders might then run the risk that their funding agreements were void for champerty. Champerty is a rule of public policy which proscribes the improper support of litigation by an otherwise disinterested party in return for a division of the spoils. The common law condemns champerty because of the abuses to which it may give rise. The champertous maintainer might be tempted, for his own personal gain, to inflame damages, suppress evidence or suborn witnesses. The appellate court rejected this argument, holding: "champerty involves behaviour likely to interfere with the due administration of justice. Litigation funding is an accepted and judicially sanctioned activity perceived to be in the public interest."

The Funders who advanced funds to enable Excalibur to furnish court-order security for costs argued that, having part-satisfied the order for costs against Excalibur, they should face no further liability. Those funders had not assumed the risk of being made liable to meet costs in an additional amount in excess of the amount advanced for that specific purpose. The Court of Appeal rejected that argument as well, holding that (i) the provision of funds to provide security for costs is not the equivalent of a payment of costs ordered at the end of a case. Rather it is a form of funding the claim in exchange for a return—in effect, an investment (ii) no distinction is made between categories of costs—all funds advanced are used in pursuit of the common purpose and (iii) it is incorrect to consider that these funders had already discharged a liability to the Claimant. The proper analysis is that the Funders had enabled the Claimant to discharge, *pro tanto,* its own liability to the Defendants.

Finally, three funders who had not entered into a direct funding agreement with Excalibur but instead provided the funds contracted to be provided by their associated companies on back-to-back terms (i.e., on the basis that in return for their advance, they would receive the rewards in the event of success) argued that that to treat them as funders impermissibly pierced the corporate veil. Having set out the funders commitments and expected investment returns in the judgment, the judge rejected this argument, holding that (i) the court looks to the economic reality of the situation, (ii) the making of a non-party costs order does not amount to an enforcement of legal rights and obligations to which the doctrine of corporate personality is relevant, and (iii) if an order were available only against a funder who had entered into a contractual relationship with the funded litigant, funders could insulate themselves from exposure by use of special purpose vehicles.

The Court of Appeal ruling may act to greatly increase the liability exposure of litigation funders in unsuccessful cases. As a result, funders may be minded to revise assumptions in their funding models, increase due diligence as to the merits of claims or take an interventionist approach to the litigation process.

Should Funders Revise Assumptions in Their Funding Models Which Estimate Costs Prospectively and on a Standard Basis?

The Court of Appeal was clear that to award costs against an unsuccessful party on an indemnity scale is a departure from the norm. In assessing the funding model, accordingly, one considers whether the case at issue falls outside the norm. Excalibur was such an exceptional case. "Countless" factors militated strongly in favor of indemnity costs against the Funders, including the unmeritorious claims and poor conduct of the Claimant and its legal representatives, Clifford Chance. Claimants counsel later settled the Funders negligence suit for an undisclosed sum. Circumstances taking a case out of the norm have included reliance on deficient expert evidence, the pursuit of serious, wide-ranging allegations of dishonesty by the Defendant (in one case, before HM Treasury, Parliament and the Governors of the Bank of England) or of speculative, grossly exaggerated and opportunistic claims.

Should Funders Increase Due Diligence as to the Merits of Claims?

The due diligence undertaken by the Funders in this case was certainly inadequate. However, the Court is unlikely to consider it necessary to investigate whether a funder knew or ought to have known of the egregious

features of the case which give rise to indemnity costs. An enquiry into the adequacy of a funder's due diligence would be unsatisfactory and often impossible—funded parties are disinclined to waive privilege over relevant communications. Any enquiry into the adequacy of the due diligence undertaken would also give rise to the prospect of undesirable satellite litigation. The judge did however, make clear that rigorous analysis of the claim is expected of a responsible funder. In addition, on-going review of the litigation by lawyers independent of those conducting the litigation, *a fortiori* those conducting it on a conditional fee agreement, seems "often essential in order to reduce the risk of orders for indemnity costs being made against the unsuccessful funded party."

Should Funders Take a More Interventionist Approach to the Litigation Process?

The judge was sensitive to the need to ensure that, "commercial funders who provide help to those seeking access to justice which they could not otherwise afford are not deterred by the fear of disproportionate costs consequences if the litigation they are supporting does not succeed." Accordingly, while this decision should not send a chill through the litigation funding industry, it provides important guidance on the extent of funders' liability: (i) commercial funders will ordinarily be required to contribute to costs on the same basis as their funded party, even where those costs are calculated on a higher indemnity basis; (ii) a funder may be accountable for wrongdoing by those it has funded engaged or enlisted; (iii) a costs order may apply to a parent 'funding the funder'; and (iv) on-going review by independent lawyers should reduce the risk of an indemnity costs order against an unsuccessful funded party. Ultimately, funders should be prepared to follow the fortunes of their funded party. Q

PRACTICE AREA NOTES

White Collar Litigation Update

OFAC's Revised FAQs Regarding Iranian Sanctions: The Impact for Non-U.S. Companies Seeking to Do Business with Iran. On October 7, 2016 the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") revised its Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions Under the Joint Comprehensive Plan of Action on Implementation Day (the "FAQs"). While some commentators initially described the revisions as an easing of sanctions, OFAC itself has insisted that the revisions do not change, but simply clarify pre-existing rules. A close reading of the October 7 revisions reveals that they are consistent with and do not alter the rules under which non-U.S. companies have been operating since most secondary sanctions against Iran were lifted earlier this year.

The revised FAQs address three key issues that are of critical importance to any company seeking to do business in or with Iran: (1) the use of U.S. dollars in transactions involving Iran; (2) doing business with counterparties that are minority-owned or wholly or partially controlled by persons or entities on the OFAC Specially Designated Nationals List (the "SDN List"); and (3) the due diligence required when transacting with Iranian counterparties.

1. FAQs regarding U.S. dollar transactions by non-U.S., non-Iranian persons. With respect to the use of U.S. dollar denominated transactions by foreign financial institutions, the revised FAQs provide that non-U.S. financial institutions (including foreign-incorporated subsidiaries of U.S. financial institutions) may process transactions denominated in U.S. dollars or maintain U.S. dollar-denominated accounts that involve Iran, provided that such transactions or account activities do not involve, directly or indirectly, the United States financial system or any United States person, and do not involve any person on the SDN List. However, non-U.S. financial institutions, including foreign-incorporated subsidiaries of U.S. financial institutions, must continue to ensure that they do not process U.S. dollar-denominated transactions involving Iran through the U.S. financial system or otherwise involve U.S. financial institutions (including their foreign branches), given that U.S. persons continue to be prohibited from exporting goods, services (including financial services), or technology directly or indirectly to Iran.

The revised FAQs thus provide some comfort to non-U.S. financial institutions that can engage in U.S. dollar transactions involving Iran, provided that they have sufficient U.S. dollars in reserve to process the transaction outside of the U.S. financial system without the need to clear the transaction through a U.S. correspondent bank. Non-U.S. financial institutions must remain vigilant, however,

and should have appropriate systems and controls in place to ensure that they do not route transactions involving Iran to or through the U.S. financial system unless the transactions are exempt from regulation or authorized by OFAC.

2. Foreign persons doing business with non-SDN listed entities that are controlled or minority-owned by Iranian SDN listed entities. OFAC's Fifty Percent Rule, in place since August 2014, provides that any entity owned in the aggregate, directly or indirectly, fifty percent or more by one or more sanctioned persons is itself considered to be a sanctioned person. Under the rule, the property and interests in property of such an entity are blocked regardless of whether the entity itself is listed on the SDN List.

The revised FAQs provide that "[i]t is not necessarily sanctionable for a non-U.S. person to engage in transactions with an entity that is not on the SDN List but that is minority owned, or that is controlled in whole or in part, by an Iranian or Iran-related person on the SDN List. However, OFAC recommends exercising caution when engaging in transactions with such entities to ensure that such transactions do not involve Iranian or Iran-related persons on the SDN List."

OFAC's hedged language and warning to tread carefully when engaging in such transactions shows that this remains an area fraught with risk. While it is "not necessarily sanctionable" for non-U.S. companies to do business with a counterparty that is controlled or minority-owned by an SDN-listed entity, such control or minority-ownership is at least a red flag that requires enhanced due diligence and compliance controls.

3. Due diligence required when contracting with Iranian counterparties. Finally, the revised FAQs discuss OFAC's due diligence expectations for non-U.S. persons doing business with Iranian counterparties. According to the revised FAQs, screening the names of Iranian counterparties against the SDN List is "a step that would generally be expected, but that is not necessarily sufficient." Beyond that, OFAC offers little guidance on what due diligence would be sufficient, other than to state that non-U.S. persons should consult local regulators regarding due diligence expectations in domestic jurisdictions, and should ensure his or her due diligence procedures conform to his or her internal risk-assessment and overall compliance policies, which should be based on the best practices of his or her industry and home jurisdiction. While the OFAC considers it a best practice for non-U.S. financial institutions to perform due diligence on their own clients, there is no expectation for non-U.S. financial institutions to repeat the due diligence their customers performed on an Iranian customer, "unless the non-U.S. financial institution has reason to believe that those processes are insufficient."

Conclusion. Although OFAC claims that the updated FAQs are intended "to provide further clarity on the scope of the sanctions lifting that occurred on Implementation Day of the [Joint Comprehensive Plan of Action]," the FAQs in fact leave non-U.S. businesses facing a degree of uncertainty (and thus, risk) when entering into transactions with Iran. Companies looking to do business with Iranian counterparties must proceed with caution and ensure they have established sufficient compliance policies and controls to prevent possible violations.

Class Action Update

Spokeo's Impact: A Potent but Mercurial Class Action Gatekeeper. The Supreme Court's May 2016 decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540(2016), *as revised* (May 24, 2016), promised to rein in the wave of class actions premised on "no injury" statutory violations, where the threat of crippling aggregated damages prompted numerous significant settlements. *Spokeo* held that a "bare procedural violation" of a statute cannot establish Article III standing, and thus appeared to preclude lawsuits premised on technical violations of federal statutes where no harm resulted. In the six months since *Spokeo* issued, the decision has had an undeniable effect in limiting such claims. But lower court interpretations have not been uniform, which means that, for now, venue might matter.

In *Spokeo*, the plaintiff alleged that a "people search engine" that generated credit report information had been disseminating inaccurate personal data in violation of Section 1681(b) of the Fair Credit Reporting Act (FCRA). Spokeo challenged whether these allegations sufficiently pleaded the "injury in fact" required under Article III of the Constitution. The Supreme Court remanded on the sufficiency of those specific allegations, but clarified important aspects of the injury-in-fact analysis in the context of statutory violations.

First, the Court concluded that not all harms statutorily defined by Congress rise to the level of constitutional injury in fact. The Court emphasized that concreteness and particularization are distinct requirements. *Spokeo* at *6. To be "concrete," an injury "must be '*de facto*'; that is, it must actually exist." *Id.* at *7 (internal citation omitted). The adjective

"concrete" is "meant to convey the usual meaning of the term—'real,' and not 'abstract.'" *Id.* Although the Supreme Court agreed that Congress plays a role in identifying "intangible" harms that should be actionable, the harm or risk of harm identified must still constitute a concrete injury in fact to confer standing. *Id.* at *7. Article III is not "automatically satisfie[d] . . . whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Id.*

Second, the Supreme Court emphasized that the mere violation of a *procedural* requirement in place to safeguard congressionally recognized harms (even a harm that is sufficiently concrete and particularized) does not independently constitute a cognizable harm. Rather, procedural breaches confer constitutional standing only when they separately entail "a degree of risk sufficient to meet the concreteness requirement." *Id.* at *8.

Following *Spokeo*, defendants facing class actions based on alleged statutory violations were quick to file or renew Article III standing challenges. Of the more than 150 opinions that have since issued, courts found a lack of standing in about 40% of the cases. Much of the variance in results can be attributed to understandable differences in the plausibility of the actual harm allegations, but even among the relatively few of these cases that have already made their way through the Circuit Courts, it is sometimes difficult to identify principled distinctions.

Some courts have not hesitated to conclude that the plaintiff failed to identify "concrete harm" resulting from the defendant's alleged statutory violation. For example, in *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016), the plaintiff asserted a violation of the Consumer Protection Act based on Urban Outfitters' practice of collecting customers' zip codes while processing credit card transactions. The D.C. Circuit, relying on *Spokeo*, concluded that where the plaintiff admitted its only injury was being "asked for a zip code when under the law they should not have been," the plaintiff had not alleged the requisite "risk of real harm." *Id.* The Eighth Circuit reached a similar conclusion in *Braitberg v. Charter Communications, Inc.*, 836 F.3d 925, 927-30 (8th Cir. 2016), dismissing allegations that a cable provider failed to destroy the plaintiff's personal information in violation of a statute where the plaintiff "identifie[d] no material risk of harm from the retention."

However, other courts have seized on the fact-intensive nature of the "injury-in-fact" inquiry and the lack of clear guidance from the Supreme Court and have found standing even when confronted with similar fact patterns. The Sixth Circuit in *Galaria v. Nationwide Mutual Insurance Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016), ruled that the plaintiffs need not wait for their information to actually be misused to claim standing. "[A]lthough it might not be literally certain that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm." (internal citations and quotations omitted); *see also Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 693 (7th Cir. 2015) (finding standing in a data breach case because, "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.") Likewise, in *Strubel v. Comenity Bank*, No. 15-528-CV, 2016 WL 6892197, at *5 (2d Cir. Nov. 23, 2016), the Second Circuit found standing where plaintiff alleged that her bank failed to give her proper notice of certain aspects of her credit card agreement. According to the Second Circuit, because a "consumer who is not given notice of his obligations is likely not to satisfy them," failure to provide required notice necessarily affects plaintiff "in a personal and individual way." *Id.*

In the near term, this lack of consensus means the pleading stage battles over *Spokeo* will rage on. Plaintiffs will likely seek to file in circuits they perceive as more favorable venues until greater clarity and consistency emerges. But even in just six months, *Spokeo* has played a profound gatekeeping role with respect to this species of class action, which exposes companies of all types to massive statutory damages.

Quinn Emanuel Elects Thirteen New Partners

Quinn Emanuel Urquhart & Sullivan, LLP announced the election of thirteen new partners effective January 1, 2017. Managing Partner John B. Quinn said: "We are very pleased that we were able to elect thirteen outstanding new partners. It is a diverse group, including five women. Most of them have been with us since they graduated from law school."

The newly elected partners are as follows:

Julia Beskin is based in the firm's New York office. Her practice is complex commercial litigation with an emphasis on cases involving securities, structured financial products, M&A, corporate governance, and banking. She also has extensive experience representing clients in regulatory investigations. Julia received a B.A. *with high distinction* in Political Science and History from the University of Toronto, and a J.D. *with honors* from the University of Toronto.

David M. Cooper is based in the firm's New York office. He is a member of the firm's appellate practice and focuses on brief-writing and oral argument in complex commercial litigation. He received a B.A. in economics, *cum laude*, from Harvard College and a J.D. from Stanford University, where he graduated first in his class. David clerked for Justice Anthony Kennedy of the U.S. Supreme Court and Judge Merrick Garland of the U.S. Court of Appeals for the D.C. Circuit.

Laura Fairneny is based in the firm's New York office. She does patent litigation related to pharmaceuticals, medical devices, and biotechnology. Laura received a J.D. from the University of Virginia School of Law, where she served on the Editorial Board of the *Virginia Law Review*. She also received a B.A. with *high distinction* in both Biology and Political and Social Thought from the University of Virginia and clerked for the Honorable Legrome D. Davis of the U.S. District Court for the Eastern District of Pennsylvania.

Keith Forst is based in the firm's Washington, D.C. office. Keith is a trial lawyer that represents clients across a wide range of complex commercial matters, including intellectual property, energy and class action litigation, and international arbitration. Keith received a Bachelor of Science in Chemical Engineering, *magna cum laude*, from the New Jersey Institute of Technology, and a J.D. from Georgetown University Law Center.

Andrew M. Holmes is based in the firm's San Francisco office. He does technology-based litigation with an emphasis on patent, copyright, and other intellectual property disputes, including proceedings before the Patent Trial and Appeal Board. Drew graduated from the University of California, Berkeley with a degree in molecular and cell biology, and received his J.D., *magna cum laude*, from the University of California, Hastings College of the Law, where he was Senior Production Editor of the *Hastings Law Journal*.

Khaled Khatoun is based in the firm's London office. He does complex, high value commercial litigation and arbitration, often with a significant cross-border element. He received an M.A. (*first class honours*) from Edinburgh University, where he graduated top of his year, and a *distinction* from BPP Law School.

Valerie A. Lozano is based in the firm's Los Angeles office. She is a trial lawyer focused on complex business litigation with an emphasis on intellectual property disputes. Valerie has extensive trial experience in state and federal courts throughout the country. She holds a B.B.A. in finance, *with honors*, and a J.D. ,*with honors*, from the University of Texas.

Brian E. Mack is based in the firm's San Francisco office. He does technology-based litigation with an emphasis on patent, trade secret, and other intellectual property disputes. Brian received a B.A. in computer science and physics from Hamilton College, a M.S. in electrical engineering from Columbia University, and a J.D., *cum laude*, from Fordham University, where he was Editor of the *Fordham Law Review*.

Rachael L.B. McCracken is based in the firm's Los Angeles office. Rachael does complex commercial litigation with an emphasis on securities and antitrust disputes and trial practice. She graduated with a B.A., *summa cum laude,* and Phi Beta Kappa from Amherst College and received a law degree from New York University, where she was in the Order of the Barristers and an Ostrow Scholarship Recipient.

Sami H. Rashid is based in the firm's New York office. Sami has extensive experience representing both corporate plaintiffs and defendants in antitrust and other complex commercial litigation, including class actions. Sami received a B.A. in Government from Cornell University, an M.A. in Chinese Studies, *with*

distinction, from the University of London (School of Oriental and African Studies), and a J.D, *cum laude*, from New York University School of Law.

Matthew R. Scheck is based in the firm's Los Angeles office. He does complex corporate bankruptcies, bankruptcy-related litigation, and commercial litigation. Matthew received a B.A. in psychology from Washington University in St. Louis and a J.D., *magna cum laude*, from Boston University School of Law, where he was Note Development Editor of the *Boston University Law Review*. Prior to joining the firm, Matthew clerked for Judge Robert D. Drain of the United States Bankruptcy Court for the Southern District of New York.

Ellyde R. Thompson is based in the firm's New York office. She has extensive experience litigating disputes relating to the energy sector, copyright and trademark law, commercial matters, and constitutional law. Ellyde practices regularly in federal and state appellate courts. She received a B.S. in Journalism from the Medill School of Journalism at Northwestern University. Ellyde graduated *magna cum laude* from Fordham University School of Law and clerked for the Honorable Betty Binns Fletcher of the U.S. Court of Appeals for the Ninth Circuit.

Lance Yang is based in the firm's Los Angeles office. He specializes in technology-based litigation with an emphasis on patent, trade secret, and other intellectual property disputes. Before attending the University of Pennsylvania Law School, he spent five years as an engineer and received a Masters Degree from Stanford University in Electrical Engineering. He also holds an LL.M. from Tsinghua University and is admitted to the United States Patent and Trademark Office.

Leading International Arbitration Specialist Isabelle Michou Joins Paris Office

Isabelle Michou has joined the firm as a partner based in the Paris office. Isabelle was previously a partner at Herbert Smith Freehills, where she was head of that firm's Paris office disputes practice. She specializes in international arbitration and international law, and has represented a broad array of clients including sovereign states and large corporations in many industries, such as hospitality, oil and gas, aerospace and large infrastructure projects. Isabelle has advocated in all the major arbitration forums and under all the major arbitration rules including the International Chamber of Commerce (ICC), International Centre for Settlement of Investment Disputes (ICSID), London Court of International Arbitration (LCIA), the Stockholm Chamber of Commerce (SCC), and in ad hoc arbitrations under the rules of the United Nations Commission on International Trade Law (UNCITRAL).

Leading Patent Trial Lawyer Brian Biddinger Joins New York Office

Brian P. Biddinger has joined the firm as a partner in its New York office from Ropes & Gray, where he was also a partner. Brian is an experienced trial lawyer who specializes in patent litigation matters in district court, in which he has tried cases across the country, the International Trade Commission, and the Patent Trial and Appeal Board. He counsels clients whose businesses are in a variety of technical fields, including automotive, wireless communications, consumer products, video games, microprocessors, flash memory, and medical devices. He also has extensive experience representing clients in *inter partes review* and ex parte re-examination proceedings. He has argued multiple times before the PTAB and has particular expertise coordinating the successful use of patent office challenges with pending district court litigation.

VICTORIES

RICO Victory for Investment and Management Company

The firm recently secured a complete victory over a dangerous and relentless adversary in the District of Delaware. In 2008, our client Ray Mirra, an entrepreneur in the specialty pharmaceutical industry, entered into a separation agreement with his business partner Gigi Jordan, which resulted in Ms. Jordan receiving $50 million. Two years later, Ms. Jordan killed her 10-year-old autistic son in a suite at the Peninsula Hotel in Manhattan by force-feeding him a mimosa cocktail laced with an extreme dose of painkillers. Ms. Jordan was quickly arrested for the crime and put on trial in Manhattan. In concocting her criminal defense at trial, Ms. Jordan formed an outrageous narrative that she had killed her son due to an extreme emotional disturbance caused by her belief that Mr. Mirra and all of their former joint business associates had formed a racketeering enterprise for the purpose of stealing hundreds of millions of dollars from her, and that Mr. Mirra was trying to kill her to cover up the theft. She would later tell this tale to Dr. Phil and the New York Daily News (among other media outlets), harming Mr. Mirra's good name on the way to her ultimate conviction for killing her son. Also in the process of spreading this lie, she filed a $250 million federal RICO complaint against Mr. Mirra and several of his companies and employees.

Quinn Emanuel moved to dismiss this baseless—though potentially devastating—RICO suit in September 2014. The firm's argument centered around the theory that if Ms. Jordan had actually been defrauded (which she had not), the schedules of assets in the business separation agreement should have excited "storm warnings" sufficient to put Ms. Jordan on inquiry notice of her claims in early 2008, triggering the statute of limitations period. While this theory would ultimately be adopted by the district court when it granted the firm's motion two years later, the parties were ordered to proceed with discovery in the meantime. What followed was a battle involving incredible volumes of documents, contentious depositions, and discovery disputes at every turn. Quinn Emanuel prevailed at every aspect of the process, and ultimately built a strong factual record against Ms. Jordan, which allowed the court to comfortably rule on the firm's motion to dismiss. The motion was granted with prejudice on August 31, 2016, on both statute of limitations grounds and due to the insufficiency of the RICO claims. While Ms. Jordan continues to pursue an appeal, this victory proved to be a tremendous help to Mr. Mirra in both clearing his good name and getting back to what he does best: building businesses that provide life-saving drugs and medical treatment to patients facing rare disorders.

Bet-the-Company Victory in Delaware Supreme Court

Earlier this month, Quinn Emanuel won an appellate victory in Delaware Supreme Court that affirmed a bet-the-company trial victory. In *Quadrant Structured Products Company, Inc. v. Vertin, et al.* (Case No. 210, 2016), plaintiff Quadrant Structured Products Company, Inc. ("Quadrant") sued our clients Athilon Capital Corp. and Athilon's Board of Directors ("Athilon"), seeking an order requiring Athilon not only to pay damages of hundreds of millions of dollars—but also to liquidate its assets and shut its business down entirely. Quadrant, a noteholder, argued that Athilon was insolvent when it made transfers of assets to an affiliated entity and embarked on a business strategy that involved investing in "risky" securities. Quadrant argued that in so doing, Athilon's Board breached the terms of the indenture governing the notes held by Quadrant, engaged in actual and constructive fraudulent transfers, and breached fiduciary duties owed to Athilon's creditors.

Following a five day bench trial, the Delaware Chancery Court issued a post-trial decision that dismissed all of Quadrant's claims. Vice Chancellor Laster's post-trial decision ruled that Athilon's challenged conduct complied with the terms of the indenture, were not actual or constructive fraudulent transfers, and that Quadrant lacked standing to assert the claims for breach of fiduciary duty because when the challenged transactions took place, Athilon was, in fact, solvent. The trial court decision is described in detail in our Firm's January 2016 Business Litigation Newsletter.

On appeal, Quadrant challenged the trial court's rulings, again seeking to force Athilon to shut its business down.

After an *en banc* oral argument, the Delaware Supreme Court summarily affirmed the trial court's decision.

This decision preserved Athilon's trial success, vindicated Athilon's business strategy that Quadrant challenged, and finally terminated Quadrant's five-year long effort to force Athilon to go out of business.

Victory for Pfizer in Trade Secrets Jury Trial

The firm recently won an important victory for Pfizer Inc. in a trade secret misappropriation case tried in California state court.

In 2000, Pfizer conducted a small clinical trial aimed at obtaining approval from the Food and Drug Administration ("FDA") to market a then-promising new COX-II pain medication, Bextra, for use in a surgical setting. Pfizer hired plaintiff San Francisco-based non-profit Ischemia Research and Education Foundation ("IREF") to assist in this clinical trial and, in so doing, licensed IREF's trade secret databases which contained detailed observations of thousands of patients who had undergone coronary artery bypass graft ("CABG") surgery. After obtaining inconclusive safety results, Pfizer planned a second, larger clinical trial in the same CABG population. IREF again offered to license its databases and to provide its network of doctors who could participate in the study. Pfizer declined to license the IREF databases, but hired IREF for other services, including the appointment of IREF's lead biostatistician, Dr. Ping Hsu, to the trial's data safety monitoring committee. Following this second trial, IREF's founder, CEO, and now lone board member, found analyses of IREF's databases allegedly done in connection with the clinical trial on Dr. Hsu's computer at IREF's offices. Dr. Hsu was placed on leave, and within minutes of DHL delivering a document preservation notice, he booted his laptop, burned data to CDs (which were never seen again), deleted the burn logs, and erased hundreds of files from his computer.

IREF sued Pfizer and Dr. Hsu for trade secret misappropriation in 2004. The case was tried in 2008, and the jury found that Pfizer had directly misappropriated IREF's trade secrets, had conspired with Dr. Hsu to do so, and that Dr. Hsu was Pfizer's agent. With interest, the judgment was almost $60 million. The Court subsequently granted Pfizer's motion for a new trial.

Quinn Emanuel was retained and successfully bifurcated the case twice, once to try liability against Pfizer only, and a second time to isolate Pfizer as the sole defendant in a damages trial. Following appeal of the new trial order and remand of the case, a seven-week liability trial commenced in 2015. Through persuasive motions *in limine* and bench briefs, we successfully excluded highly inflammatory evidence, including that of Dr. Hsu's document destruction. By the end of the case, IREF's lawyers were so worried about having over-reached that they dismissed the direct liability and conspiracy claims, leaving only agency claims to go to the jury. Of the 159 trade secret computer files at issue, the 2015 jury found that Dr. Hsu had misappropriated only seven while acting within the scope of his agency for Pfizer.

IREF's lawyers withdrew and new counsel substituted in to try the damages phase. Despite the limited liability findings, IREF insisted the case was still worth $55 million, which, after interest, put Pfizer at risk for over $100 million. Following strategic motions *in limine*, IREF's damages theory was narrowed and its damages claim reduced to $29 million. The damages trial lasted nearly three weeks. Notwithstanding the liability verdict against Pfizer, Quinn Emanuel succeeded in convincing the jury that Pfizer had not acted wrongfully and that the misappropriation by its agent resulted in only nominal unjust enrichment, not the windfall IREF sought. After having the case for less than 24 hours, the jury returned a verdict of $165,000.

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 650 lawyers — the largest in the world devoted solely to business litigation and arbitration.
- As of January 2017, we have tried over 2,500 cases, winning 88% of them.
- When we represent defendants, our trial experience gets us better settlements or defense verdicts.
- When representing plaintiffs, our lawyers have garnered over $51 billion in judgments and settlements.
- We have won five 9-figure jury verdicts.
- We have also obtained twenty-seven 9-figure settlements and fourteen 10-figure settlements.

LOS ANGELES
865 S. Figueroa St.,
10th Floor
Los Angeles, CA 90017
+1 213-443-3000

NEW YORK
51 Madison Ave.,
22nd Floor
New York, NY 10010
+1 212-849-7000

SAN FRANCISCO
50 California St.,
22nd Floor
San Francisco, CA 94111
+1 415-875-6600

SILICON VALLEY
555 Twin Dolphin Dr.,
5th Floor
Redwood Shores, CA 94065
+1 650-801-5000

CHICAGO
500 W. Madison St.,
Suite 2450
Chicago, IL 60661
+1 312-705-7400

WASHINGTON, D.C.
777 6th Street NW,
11th Floor
Washington, DC 20001
+1 202-538-8000

HOUSTON
Pennzoil Place
711 Louisiana St.,
Suite 500
Houston, TX 77002
+1 713-221-7000

SEATTLE
600 University Street,
Suite 2800
Seattle, WA 98101
+1 206-905-7000

TOKYO
NBF Hibiya Bldg., 25F
1-1-7, Uchisaiwai-cho,
Chiyoda-ku
Tokyo 100-0011
Japan
+81 3 5510 1711

LONDON
One Fleet Place
London EC4M 7RA
United Kingdom
+44 20 7653 2000

MANNHEIM
Mollstraße 42
68165 Mannheim
Germany
+49 621 43298 6000

HAMBURG
An der Alster 3
20099 Hamburg
Germany
+49 40 89728 7000

MUNICH
Hermann-Sack-Straße 3
80331 Munich
Germany
+49 89 20608 3000

PARIS
6 rue Lamennais
75008 Paris
France
+33 1 73 44 60 00

MOSCOW
St. Petersburg Tower,
"Capital City" Complex
"Moscow City" Business Center
8, Presnenskaya Nab., Bld 1,
Floor 19, Office 193
Moscow, 123317
Russia
+7 499 277 1000

HONG KONG
1307-1308 Two Exchange Square
8 Connaught Place
Central Hong Kong
+852 3464 5600

SYDNEY
Level 15
111 Elizabeth Street
Sydney, NSW 2000
Australia
+61 2 9146 3500

BRUSSELS
Rue Breydel 34
1040 Brussels
Belgium
+32 2 416 50 00

ZURICH
Dufourstrasse 29
8008 Zürich
Switzerland
+41 44 253 80 00

SHANGHAI
Level 20, The Center
989 Changle Rd
Shanghai 200031
+86 21 5117 5859

Prior results do not guarantee a similar outcome.