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

April 2023

quinn emanuel

quinn emanuel urquhart & sullivan, llp | business litigation report

atlanta | austin | beijing | berlin | boston | brussels | chicago | dallas | 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

Chatbots and Privacy Claims

In 2022 there was a wave of class action litigation brought under state wiretapping laws, including the California Invasion of Privacy Act (CIPA), against website operators that use chat features and session replay software. *See, e.g.*, Claburn, Thomas, *Intel accused of wiretapping because it uses analytics to track keystrokes, mouse movements on its website*, The Register (available at Intel accused of wiretapping because it uses analytics to track keystrokes, mouse movements on its website • The Register). This type of litigation is also present in other states, including Florida and Pennsylvania. A number of plaintiffs' attorneys who specialize in class action litigation have seized on CIPA section 631 claims. The number of such cases, with virtually identical "cookie cutter" complaints, has exploded.

These actions have been spurred in part by a recent unpublished Ninth Circuit decision in *Javier v. Assurance IQ, LLC*. In *Javier*, the Ninth Circuit reversed a district court's dismissal of a CIPA claim and held that retroactive consent is not a viable defense. However, *Javier* did not hold there *was* a violation of CIPA based on the allegations, nor did the court touch on any of the defendant's other defenses.

Website operators that utilize chat features and session replay technology face increased litigation exposure. Nonetheless, they have a number of defenses and options available to them. This article will explore the legal landscape concerning CIPA claims in the context of session replay software and chatbot technology, and strategies to reduce risk and

(continued on page 2)

INSIDE

Quinn Emanuel Opens Office in Beijing, Its Second in Mainland China

The firm announced an expansion and strengthening of its China practice with the launch of an office in Beijing, its second office in mainland China. The firm's Shanghai office opened in 2016.

The step comes in the wake of significant growth for the firm's China practice over the past decade. Since opening in Hong Kong and Shanghai, Quinn Emanuel has achieved extraordinary results for numerous leading Chinese companies and individuals in their most high-stakes and challenging disputes.

Quinn Emanuel Partners Named 'Litigators of the Week' for Victory on Behalf of Tesla

Partners Alex Spiro, Asher Griffin and Senior Counsel Kathleen Sullivan have been named 'Litigators of the Week' by The American Lawyer after convincing a federal jury to award damages that were 98% lower than an earlier damage verdict against our client Tesla.

Department of Justice Veteran Michael Shaheen Joins Quinn Emanuel

Michael Shaheen, one of the nation's leading False Claims Act (FCA) litigators, has joined the firm as a partner. Shaheen, formerly a partner at Crowell & Moring, will be based in the Washington, DC office, and will become Co-Head of the new False Claims Act Practice and join the Investigations, Government Enforcement & White Collar Criminal Defense Practice as well as the Health Care Litigation Practice.

to respond to such claims.

What is CIPA and what is the basis for the claims? The CIPA, section 630 *et seq.*, was enacted in 1967 and prohibits recording and eavesdropping on private communications. Its purpose is "to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 769 (2002). Section 631(a) of California's Penal Code provides for civil in addition to criminal liability for "wiretapping," and states as follows:

> (a) Any person [1] who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [4] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . .

The Supreme Court of California has distilled this down to "three distinct and mutually independent patterns of conduct: intentional wiretapping, wilfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities." *Tavernetti v. Superior Court of San Diego Cty.*, 583 P.2d 737, 741 (Cal. 1978). Under section 631(a), if a person secretly listens to another's conversation, the person is liable. *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985). A prevailing plaintiff is entitled to recover the greater of the following: five thousand dollars per violation or three times the amount of actual damages, if any. Cal. Penal Code § 637.2(a). Courts have held the statute does not require proof of actual damages.

In *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), the Ninth Circuit addressed a CIPA section 631(a) action in which the plaintiffs alleged Facebook improperly used plug-ins to track logged-out users' browsing histories when they visited third-party websites and then compiled those browsing histories for sale to advertisers. The Ninth Circuit held that in the context of forwarding and duplication of "GET requests" to Facebook's servers, Facebook did not qualify for the "party exemption"—i.e., an exemption from CIPA liability for a person who is a party to the communication. *Id.* (citing *Warden v. Kahn*, 99 Cal. App. 3d 805 (1979)). The Ninth Circuit emphasized that only third parties can wiretap communications (not the actual parties to the communication), but concluded that where an entity surreptitiously duplicates transmissions between two parties, it does not qualify for the exemption.

What technology is at issue? The new wave of wiretapping cases center around technology that is commonly-used across websites. Session-replay technology collects data concerning on-website keystrokes and mouse movements such as clicking, scrolling, swiping, and typing. A video is then created of the website visitor's interactions with the website. The visitor's data, including date and time of visit, IP address, browser and operating system, and geographic location may be recorded. If a visitor enters personally identifiable information—for example, to purchase a product using a credit card—that information may also be recorded. Typically, a website operator uses a software vendor's code to capture the website interactions, which can then be reviewed by viewing the "video" of the website interactions.

The more recent wave of actions further allege violations based on a website's use of a virtual chatbot, which permits a website visitor to engage in a text conversation with a virtual assistant or customer service representative. The plaintiffs in these actions allege the website operator defendants have "covertly" embedded code to record "transcripts" of conversations and allow a third-party vendor to obtain and store these chat communications. This, plaintiffs contend, constitutes a violation of state wiretapping laws based on the involvement of the third-party vendor in providing the underlying chat service or video recording. In turn, the plaintiffs allege the website operators have aided and abetted the violation through use of the third-party technology vendor. The first prong of section 631(a) has been considered to apply only to telegraph or telephone allegations, *see Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1135 (E.D. Cal. 2021) (noting "overwhelming weight of authority" adopting interpretation that clause applies only to wiretapping of a "telegraph or telephone"), and the third prong applies only if a plaintiff alleges an attempt to use or communicate the information.

The application of the wiretapping act might be considered an odd fit in this context. At the threshold, plaintiffs are attempting to apply the act to a person's interaction with a public website. Compare this to the secretive listening-in to a private telephone conversation

which the wiretap act was designed to prohibit. *See, e.g.*, *Ribas*, 38 Cal. 3d at 359 ("the legislature could reasonably have contemplated that section 631, subdivision (a), would prohibit the type of surreptitious monitoring of private conversations," where a third party monitored a husband's private conversation with his former wife). It is also questionable whether the typical user of a modern website would be surprised the website uses analytics provided by a third party.

The* Javier *Ruling. In *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022), the plaintiff sued the defendants, an online platform for life insurance quotes, Assurance IQ, LLC, and its "partner," ActiveProspect, for CIPA violations. The plaintiff alleged that ActiveProspect provided websites like Assurance with a product called "TrustedForm," a piece of javascript code that can be pasted into a form page to record keystrokes, mouse clicks, and other communications of visitors to websites, allowing a website owner to record a video of the user's interaction with the website, including any consent to being contacted. When the plaintiff visited Assurance's website, he alleged that the TrustedForm captured in real time his interaction with the website and created a video recording of that interaction. While on the website, after filling out the insurance quote questionnaire, the plaintiff affirmatively clicked on "View My Quote" to indicate his "intent to agree to th[e] website's Privacy Policy." *Javier v. Assurance IQ, LLC*, No. 20-CV-02860-JSW, 2021 WL 3669343, at *1 (N.D. Cal. Aug. 6, 2021). The plaintiff was not prompted to agree to the privacy policy until after his interaction with the website was recorded. The defendants successfully moved to dismiss on the grounds that the plaintiff had retroactively consented to the recording by agreeing to Assurance's privacy policy. In an unpublished decision, the Ninth Circuit reversed.

The Ninth Circuit first held that although "written in terms of wiretapping," section 631 applies broadly "to Internet communications;" it "makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'" *Javier*, 2022 WL 1744107, at *1 (citation omitted). The court then held that CIPA requires "the prior consent of all parties to a communication," and retroactive consent does not suffice. Because the plaintiff had alleged that he did not provide consent prior to the alleged recording, the Ninth Circuit reversed the district court's order dismissing the case. However, the Ninth Circuit expressly stated that its holding narrowly applied to the issue of consent and did "not reach [d]efendants' other arguments, including whether Javier impliedly consented to the data collection, whether ActiveProspect is a third party under Section 631(a), and whether the statute of limitations has run."

Litigation risks. Section 631(a) presents a litigation risk for any company that uses chatbot or session reply technology on its website. Even where meritorious defenses exist, there is still the threat of litigation, with its attendant costs and fees, including those required to respond to any complaint and any discovery that plaintiffs seek pending any motion to dismiss. *But see Zarnesky v. Adidas Am., Inc.*, No. 6:21-CV-540-PGB-GJK, 2021 WL 3729230, at *1 (M.D. Fla. June 10, 2021) (in session replay case, granting defendant's motion to stay discovery until the court rules on defendant's motion to dismiss, although recognizing that the situation is "rare").

There are a number of actions website operators can take in response to this litigation threat. As an initial matter, website operators can implement a system to obtain express prior consent *before* any session replay technology or chatbot use begins, for instance, by requiring website visitors to agree to a privacy policy prior to any recording. And, in order to assess the viability of any possible defenses, it is important to fully understand the functioning of any technologies used to collect, monitor, or record visitor interactions with an operator's website.

For defendants facing such wiretapping lawsuits, aside from obtaining express prior consent, a number of defenses may be available.

Implied consent. The Ninth Circuit in *Javier* explicitly left open whether implied consent could serve as a potential defense on remand. The contours of this argument have not yet been litigated, including what might qualify as sufficient implied consent. Section 631(a) prohibits conduct "without . . . consent." At least one court in the Ninth Circuit has opined that consent may be "express or implied." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021); *see* Cal. Prac. Guide Civ. Pro. Trial Claims and Def. Ch. 4(VII)-B (in context of misappropriation claim, "[c]onsent may be implied from plaintiff's action or inaction"); *Jones v. Corbis Corp.*, 815 F. Supp. 2d 1108, 1113-1114 (C.D. Cal. 2011) (actress impliedly consented to posting of "red carpet" photographs on defendant's website for sale where she knew photos would be taken and that custom and practice in entertainment industry was to widely use and disseminate such photos") (applying California law); *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994) ("[T]he plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant."); *Adler v. Community.com, Inc.*, No. 2:21-CV-02416-SB-JPR, 2021 WL 4805435, at *5 (C.D. Cal. Aug. 2, 2021) (in CIPA context the "'critical question' for determining

consent is whether the party in question 'had adequate notice' it was being surveilled."); *but see Javier v. Assurance IQ, LLC*, No. 20-CV-02860-CRB, 2023 WL 114225, at *3 (N.D. Cal. Jan. 5, 2023) (on remand, concluding defendant had not demonstrated that plaintiff continued to use the website after having constructive notice that his communications may be intercepted). Accordingly, and based on the specific allegations, if a user visits a website and is made aware that the information the user enters is being collected, recorded or processed by a third party vendor, but continues to use the website, that might be sufficient to constitute implied consent to the collecting, recording or processing of interaction information. As in other contexts, whether a consent defense will be available will likely depend on the specific facts, such as the notice provided, the content of that notice, and whether any notice is conspicuous.

Party exception. To plead a CIPA violation, a plaintiff must allege the person intercepting the communication was a third party, not a party to the communication. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 607 (explaining CIPA "contain[s] an exemption from liability for a person who is a 'party' to the communication"); *Ribas*, 38 Cal. 3d at 359 ("Section 631 was aimed at … eavesdropping, or the secret monitoring of conversations by third parties."). A number of federal district courts in California considering session replay software CIPA claims have dismissed the claims based on the party exemption. Instead, courts have concluded that these software vendors provide a service for the website operator to analyze its own data. *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021) (the vendor "provide[d] a tool … that allows [the website operator] to record and analyze its own data."); *Yale v. Clicktale, Inc.*, No. 20-CV-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) ("Clicktale is not a third-party eavesdropper. It is a vendor that provides a software service that allows its clients to monitor their website traffic."); *Johnson v. Blue Nile, Inc.*, No. 20-CV-08183-LB, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021) (same); *Williams v. What if Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022) (same). Other courts, however, have reached the opposite conclusion. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019) (involving a marketing company that partnered with e-commerce sites to intercept visitor data and create marketing databases of consumer information); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021) (where third party vendor had simultaneous access to website communications, no party exemption was applicable); *Yoon v. Lululemon United States*, 549 F. Supp. 3d 1073, 1077 (C.D. Cal. 2021) (claim "survives [a] participant exception challenge because [plaintiff] alleges that [third party] captures, stores, and interprets her real-time data—which extends beyond the ordinary function of a tape recorder."); *Javier*, 2023 WL 114225, at *5 (third party exemption did not apply because the plaintiff "pleads that ActiveProspect monitors, analyzes, and stores information about visits to Assurance's websites, and that Active Prospect can use that information for other purposes, even if Javier has not alleged that they have done so in this case . . . [which is] beyond the ordinary function of a tape recorder," but claim dismissed on statute of limitations grounds) (citation and quotation marks omitted). As one court has phrased the question, it "boils down to whether [the vendor] was an independent third party hired to eavesdrop on [the website operator]'s communications, or whether [the vendor]'s software was merely a tool that [the website operator] used to record its own communications with plaintiff." *Williams v. What if Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022); *see also Yoon*, 549 F. Supp. 3d at 1081 ("The question thus becomes, in analogue terms: is Quantum Metric a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door?").

In the session replay software context, courts that have found there was not a violation of CIPA have concluded that the allegations amounted to the latter: the vendors provide a product that "function[s] as a recorder, not an eavesdropper," for the website operator itself to collect information. *See Williams*, 2022 WL 17869275, at *3. However, complaints that include chatbot allegations may seek to avoid this argument by alleging the third party vendor is itself collecting and recording the communications that are being made to the website operator. Whether a "party" argument will be successful in defending against such claims may depend on the allegations of the complaint and the particular technology—for instance, whether the vendor provides software for chatbot functionality that is embedded code on a website, or whether a vendor itself collects, stores, and uses data, *e.g.*, *Revitch*, 2019 WL 5485330 at *1-*2. Some complaints appear aimed at getting around this argument by alleging real-time, simultaneous access to chat communications by third party vendors. Further, this area of law is still evolving. *See Javier*, 2023 WL 114225, at *5 (summarizing split).

Content. Some courts considering motions to dismiss cases premised on the use of session replay software have dismissed claims, or parts of claims, to the extent they are predicated on non-content information. Section 631(a) prohibits the unauthorized access of the contents of any communications. In analyzing the federal Wiretap Act, the Ninth Circuit has explained that the

"content" does not include "record information regarding the characteristics of the message that is generated in the course of the communication," such as "the name, address and subscriber number or identity of a subscriber or customer." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Some courts have held that, in the session replay context, CIPA claims may be subject to dismissal where the only information allegedly captured is the characteristics of a message, such as origin, date, and time information. *See, e.g.*, *Graham*, 533 F. Supp. 3d at 833; *Yale*, 2021 WL 1428400, at *3; *Johnson*, 2021 WL 1312771, at *2. At least one district court considering a section 631(a) claim based on the use of chatbot technology concluded, in contrast, that where the plaintiff alleged she shared "sensitive personal information," this was sufficient to allege that the conversations contained "more than mere record information," and thus sufficed to state a claim under section 631(a). *Byars v. The Goodyear Tire and Rubber Co.*, Case No. 5:22-cv-01358-SSS-KK, Dkt. 175 (C.D. Cal. February 3, 2023). The court concluded that a plaintiff need not "allege the exact contents of her communications" at the pleading stage. *Id.*

In transit. The second clause of section 631(a) requires that a defendant attempt to learn the contents of a communication while the communication is "in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]." In other words, this requires both that the conduct occur while a communication is "in transit" or while a communication is "being sent" or "received," and that the conduct occur within California. One district court case considering an application on an iPhone that copied content from another application held this conduct did not satisfy the "in transit" requirement because the content was obtained from "*previously-sent or previously-received* communications"—in other words, there was no allegation that the application "ever read or learned the contents of a communication while the communication was in transit, or in the process of being sent or received." *Mastel*, 549 F. Supp. 3d at 1132 (emphasis added); *see also Adler v. Community.com, Inc.*, No. 2:21-CV-02416-SB-JPR, 2021 WL 4805435, at *4 (C.D. Cal. Aug. 2, 2021); *Quigley v. Yelp, Inc.*, No. 17-CV-03771-RS, 2018 WL 7204066, at *4 (N.D. Cal. Jan. 22, 2018) ("An 'interception' only occurs if communications are "acquired during transmission, not while [ ] in electronic storage."). Whether this defense would apply to chatbot technology depends on the precise functioning of the technology and the allegations of any complaint. One district court recently concluded a plaintiff sufficiently stated a section 631(a) claim at the pleading stage by alleging the third-party service "'intercepts in real time' a website visitors' chat conversation." *Byars v. The Goodyear Tire and Rubber Co.*, Case No. 5:22-cv-01358-SSS-KK, Dkt. 175 (C.D. Cal. February 3, 2023).

Article III injury. Where the plaintiffs had not alleged they entered any personal information on a website utilizing session replay software, at least one court has held that simply recording browsing activities does not suffice for a concrete injury as required for Article III standing in federal court. *See Massie v. Gen. Motors LLC*, 2022 WL 534468, at *2 (D. Del. Feb. 17, 2022) ("Plaintiffs do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here," and rejecting argument that there was a concrete injury to plaintiffs' "interest in controlling their personal information" in these circumstances); *but see In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 597-98 (standing for CIPA claim established where plaintiffs alleged privacy harms). The applicability of this particular argument to other cases will depend on the precise allegations regarding the content of the information at issue and, of course, the venue for the action.

Other potential defenses. Other defenses may also be available depending on the case, such as any statute of limitations defense. *See Javier*, 2022 WL 1744107, at *2.

Summary. Companies should ensure they comply with wiretapping laws and get ahead of this litigation—including by fully understanding the technologies used on their websites—and should consider implementing procedures to obtain express consent.

Courts Begin To Ask Whether Decentralized Autonomous Organizations Be Held Communally Liable

Federal and state courts have recently seen an influx of lawsuits against actors and entities operating in the crypto space. Until recently, however, *who* could be a defendant charged with alleged misdeeds – including the sale of unregistered securities – has not been at issue. A few years after the rise of "Decentralized Finance," a set of recent cases promises to change this, focusing on how blockchain-based enterprises alter traditional legal conceptions of the organizations and individuals liable for actions undertaken by broad and distributed groups.

Decentralized Autonomous Organizations

Followers of the crypto space are familiar with the concept of decentralized autonomous organizations, or "DAOs." A DAO is a software-based organization whose actions are executed through smart contracts on a blockchain. Individuals and entities that own governance stakes in the DAO's operation – usually, a particular crypto token – use distributed voting, automated rules, and code to implement DAO operations. Proponents of DAOs often stress the decentralized, flat nature of the organizations' structure: decisions about particular actions that a DAO takes are generally determined by organization-wide votes, where holders of the corresponding token can vote on the proposed course of action. If the vote passes, the DAO implements that mandate autonomously, according to rules and directives encoded into one or more smart contracts. According to its proponents, this system of decentralized voting and autonomous management eliminates the hierarchies associated with traditional organizations, democratizing the DAO's operation.

The SEC's 2017 Report on The DAO

Years before DAOs began to be sued in the courts, in July 2017, the Securities & Exchange Commission ("SEC") released a report of investigation into "The DAO," one of the earliest large-scale DAOs, built on the Ethereum blockchain, offering indications of how the SEC viewed DAOs. *See* 117 SEC Docket 745 (July 25, 2017). In the case of The DAO, users could acquire DAO tokens by sending ETH tokens to The DAO, which would create and remit a proportional amount of DAO tokens to the user. The SEC's report focused on the SEC's view of how federal securities laws applied to these transactions, and, in particular, whether DAO tokens qualified as "investment contracts" and therefore securities under the test laid out in *S.E.C. v. W.J. Howey Co.*, 328 U.S. 293 (1946). After arguing that DAO tokens qualified as securities, the SEC went on to find that The DAO itself – which the SEC characterized as an unincorporated organization – was a securities issuer subject to federal securities registration requirements. But the SEC ultimately did not bring any action against The DAO or (as of yet) any other decentralized autonomous organization. As such, and as noted below, private lawsuits stand poised to test the role of DAOs in connection with federal securities laws and other legal claims in the courts.

Sarcuni v. bZx DAO

One of the first widely-publicized explicit attempts to sue a DAO came in 2022 in *Sarcuni v. bZx DAO*, No. 3:22-cv-00618 (S.D. Cal.). The allegations in *Sarcuni* arose out of a phishing scam; the plaintiffs are a group of individuals who deposited crypto tokens into a trading platform – the bZx protocol – that allowed users to lend tokens and earn interest on those loans. *Sarcuni* involves a single count of negligence, centered around alleged deficiencies in the bZx protocol's security precautions, which hackers exploited to steal millions of dollars from the protocol and its depositors.

Despite the straightforward nature of their claim, the *Sarcuni* plaintiffs faced an unusual dilemma in bringing suit: several months before the events at issue, the entities controlling the bZx protocol transitioned that control to the bZx DAO, which was in turn controlled by holders of the BZRX token. To address that dilemma, the *Sarcuni* plaintiffs are alleging that the bZx DAO functions and should be treated as a general partnership – with BZRX token holders standing in as general partners and liable under traditional partnership principles.

The specific token holders the *Sarcuni* plaintiffs named in their complaint were Kyle Kistner and Tom Bean – individuals who spearheaded the initial design and deployment of the protocol – as well as two LLCs that the complaint alleges are self-stated "investors" in the protocol that were involved in bZx's decision-making process. These defendants have moved to dismiss on a variety of grounds – some traditional, others less so. Notably, the two "investor" LLCs have argued that the *Sarcuni* Plaintiffs, having based their theory of liability primarily (if not entirely) on the LLCs' membership in the bZx DAO, cannot then allege that DAO members can be on both sides of the "v" at the same time – that is, the LLCs cannot have owed a duty to DAO member plaintiffs that are ultimately similarly-situated to the LLCs themselves since all hold governance tokens. Defendants' motions to dismiss are currently pending.

CFTC v. Ooki DAO

The Ooki DAO, a successor to the bZx DAO, also found

itself in the sights of the Commodities Futures Trading Commission ("CFTC"). In September 2022, the CFTC reached a settlement with Kistner, Bean, and bZeroX, LLC (the entity originally responsible for the operation of the DAO, also sued in *Sarcuni*). *See In the Matter of Bzerox, LLC, et al.*, CFTC No. 22-31, 2022 WL 4597664, at *10-11 (Sept. 22, 2022). But, not yet satisfied, the CFTC also filed suit in federal court against the entire Ooki DAO itself. *See CFTC v. Ooki DAO*, No. 3:22-cv-05416 (N.D. Cal., Sept. 22, 2022). In a case that has been assigned to Judge William Orrick III, neither of the DAO's co-founders nor bZeroX, LLC are named as defendants, as they have already settled. Tasked with serving the DAO itself, the CFTC attempted to serve the organization by submitting service papers through the Ooki DAO's Help Chat Box and posting notice of that service on the DAO's online forum, then moving for and receiving court approval for its "alternative service."

After Judge Orrick granted that motion, however, four non-parties – LeXpunK, the DeFi Education Fund, Paradigm Operations LP, and a16z sought leave to file amicus briefs seeking reconsideration. After a hearing on the motions, Judge Orrick ordered the CFTC to serve just one identifiable Ooki DAO token holder, specifically at least one of the Ooki DAO's co-founders (even though they were not named defendants). However, on December 20, 2022, Judge Orrick issued a detailed order rejecting the non-parties' arguments that it should not be possible to serve the Ooki DAO at all. Noting that he was facing a "case of first impression," Judge Orrick determined that the Ooki DAO, having received both actual notice and the best notice practicable under the circumstances, had been properly served. While Judge Orrick's holding addresses the question of service, his reasoning gives some insights into the Court's application of traditional legal doctrines to DAOs.

Notably, Judge Orrick concluded that the CFTC had adequately alleged that the Ooki DAO was an unincorporated association that is capable of being sued under California law. Ticking off the elements necessary to find that the Ooki DAO was an unincorporated association, Judge Orrick determined that the CFTC had alleged or shown that (i) Ooki DAO was a group of two or more persons; (ii) who had joined Ooki DAO by mutual consent; and (iii) and that the Ooki DAO had a common lawful purpose. Judge Orrick then noted that, in the Court's determination, the Ooki DAO had structured itself in such a way that it could likely only be contacted online. Emphasizing that finding, Judge Orrick concluded that service via the Ooki DAO's Help Chat Box and online forum satisfied both the requirements of California law and constitutional due process. The CFTC subsequently moved for an entry of default against the Ooki DAO, which was entered in late January.

Notwithstanding that proceedings in the CFTC lawsuit have quieted since that entry, Judge Orrick's December 20 opinion raises important considerations for those operating in the DeFi space to consider. Principal among those is that if DAOs can be served as unincorporated associations (or partnerships) then it appears possible that any token holder of a particular DAO's token could sue (or be sued by) any other holder of that token. To this end, Judge Orrick noted that the CFTC's decision to "sue the organization rather than the Token Holders individually [was] a litigation strategy the CFTC [was] permitted to make."

To be sure, notwithstanding Judge Orrick's decision on the question of effective service, issues regarding the ultimate liability of DAO entities, as well as those related to the liability of token holders who participate in DAO governance, raise thorny questions – including those related to which token holders can or should be held liable for what DAO actions. Indeed, as CFTC Commissioner Summer K. Mersinger noted in a statement dissenting from the CFTC's September 22, 2022 enforcement action against Bean, Kistner, and bZeroX, LLC, a theory of liability which would hold all voting DAO token holders liable for a DAO's actions raises a variety of line-drawing problems that may lead to inequitable results (*e.g.*, holding token holders who have exercised their voting rights liable while those that have yet to exercise not liable – regardless of whether the votes in question had anything to do with the conduct underlying any liability on the part of the DAO). *See Dissenting Statement of Commissioner Summer K. Mersinger Regarding Enforcement Actions Against: 1) bZeroX, LLC, Tom Bean, and Kyle Kistner; and 2) Ooki DAO*, (Sept. 22, 2022).

Houghton v. Leshner (and Compound DAO)

While the motions in *CFTC v. Ooki DAO* were pending, another strikingly similar case landed on Judge Orrick's desk: *Houghton v. Leshner*, No. 3:22-cv-7781 (N.D. Cal.), a class action lawsuit seeking to hold individual and entity defendants liable as general partners in the Compound DAO, a decentralized autonomous organization responsible for, *inter alia*, selling COMP tokens. Unlike the CFTC, the *Houghton* Plaintiffs also named the two co-founders of Compound Labs – the predecessor entity to the Compound DAO – and, notably, five other entities that hold COMP tokens as defendants. The *Houghton* Plaintiffs seek to hold these defendants liable under Section 12(a)(1) of the Securities Act under the theory that the Compound DAO sold unregistered securities. The Court has extended the time for the *Houghton* defendants to respond to or move to dismiss the complaint until after appointment of a lead plaintiff and lead counsel

pursuant to the Private Securities Litigation Reform Act of 1995 ("PSLRA"), 15 U.S.C. § 78u-4, *et seq*, which appointments occurred on March 13.

To be sure, Judge Orrick likely will not be the only judge or authority who may have to weigh in on this issue. The *Sarcuni* Defendants' motions to dismiss remain pending in the Southern District of California. Shortly after Judge Orrick's December 20 Order, the *Sarcuni* Plaintiffs filed a notice of supplemental authority, directing Judge Burns to the *CFTC v. Ooki DAO* Court's decision. The plaintiff in another case pending in the Eastern District of New York, *Kent v. PoolTogether*, No. 1:21-cv-6025 (E.D.N.Y.), concerning allegations that certain individuals and entities controlling a DAO were running an illegal lottery, filed a similar notice. And, taking a different tack than the non-parties in *CFTC v. Ooki DAO*, venture capital firm Haun Ventures recently submitted a petition for rulemaking urging the CFTC to clarify the obligations and liabilities of DAO members. Regardless, in the coming months we are likely to see more opinions with potentially ground-breaking implications for the cryptocurrency community.

PRACTICE AREA NOTES

Latin America Arbitration Update

From NAFTA to USMCA: U.S., Mexican, and Canadian Investors' Rights Under the USMCA

The United States-Mexico-Canada Agreement ("USMCA") entered into force on July 1, 2020, and replaced its predecessor, the North American Free Trade Agreement ("NAFTA"). Except for those investors who filed a Notice of Intent to arbitrate a claim under NAFTA ("NAFTA legacy claim") before April 2, 2023, NAFTA is no longer available for legacy claims. This is why it is important to understand the differences between NAFTA and the USMCA and the remedies still available for investors under the USMCA.

The USMCA compared to NAFTA

There are key differences between the USMCA and NAFTA that will impact an investor's substantive rights and ability to protect their foreign investment.

USMCA's Investor-State Arbitration Protections Apply Only to the U.S. and Mexico

Although the USMCA includes the United States, Mexico, and Canada, Canada did not sign on to the USMCA's Annexes 14-D and 14-E, which refer to investment disputes between an investor and an Annex Party and investment disputes related to covered government contracts. USMCA Articles 14.D.1 and 14.E.1. Therefore, under the USMCA, U.S. and Mexican nationals who invested in Canada and Canadian nationals who invested in the U.S. or Mexico will not be able to submit their investment disputes to arbitration under the USMCA. However, Canadian investors who invest in Mexico and Mexican investors who invest in Canada do have recourse to investor-state arbitration under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CP-TPP"). Because the U.S. did not sign on to the CP-TPP, this option is not available for U.S. investors in Canada or Canadian investors in the United States. Mexican nationals who invested in the U.S. and U.S. nationals who invested in Mexico will still have some access to investor-state dispute mechanism under USMCA, although with some limitations in terms of substantive protections available and preconditions that need to be satisfied for bringing a claim to arbitration. USMCA Annex 14-D.

USMCA's Investor-State Arbitration Provision Has Two Protection Schemes

USMCA's Chapter 14 protects (i) investments involving government contracts in "covered" sectors (also referred to as "covered government contracts" or "covered investments") and (ii) general investments. However, unlike the extensive protections afforded under NAFTA, the USMCA limits the substantive rights of investors based on the type of investment.

- Covered Government Contracts: Under the USMCA, the investment of a foreign investor, or local enterprise owned or controlled by the investor, who has a contract with the host state's government in a "covered sector," has broader protections than those granted to the other investors under the treaty. USMCA Annex 14-E(6)(a). Covered sectors include (1) oil and gas, (2) telecommunications, (3) transportation, (4) certain infrastructure, like roads and railways, and (5) power generation. USMCA Annex 14-E(6)(b). An investor with a covered investment may submit an arbitration claim alleging the host state breached any of its obligations to provide investors (1) the Minimum Standard of Treatment ("MST"), including fair and equitable treatment and full protection and security; (2) National Treatment; (3) Most Favored

Nation ("MFN") treatment; (4) either ***directly or indirectly*** expropriated their investment; and 5) Treatment in Case of Armed Conflict or Civil Strife. USMCA Articles 14.4, 14.5, 14.6(4), 14.7, and 14.8.

- General Investments: Under the USMCA, all other investments are considered a general investment. Such investors can submit an arbitration claim only if (1) the host state ***directly*** expropriated their investment, or (2) breached the National Treatment or MFN Treatment standards. USMCA Article 14.D.3(1)(a). Unlike NAFTA, the USMCA no longer allows investors with general investments to bring a claim for a state's violation of MST, fair and equitable treatment and full protection and security, or the host state's ***indirect*** expropriation of the investment. USMCA Article 14.6(2)(b).

In addition, while an investor with a covered investment can bring a claim for a host state's breach of MST, the UMSCA is clear that "the mere fact that a Party takes or fails to take an action that may be inconsistent with an investor's expectations does not constitute a breach of [MST]" USMCA Article 14.6.4.

Further, the USMCA also emphasizes that host states can adopt new regulations to protect legitimate public welfare objectives, even if the measure indirectly impacts an investment. Except in "rare circumstances," non-discriminatory regulatory actions designed to protect legitimate public welfare objectives will not constitute indirect expropriation. USMCA Article 14.6(2)(b).

USMCA Limits Investors' Access to Arbitration

The USMCA, unlike NAFTA, also limits investors' ability to submit an arbitration claim until they exhaust local remedies and do so within a certain time period. Unless "recourse to domestic remedies was obviously futile," the USMCA requires investors with general investments to exhaust local remedies "with respect to the measures alleged to constitute a breach" before seeking arbitration. Thus, investors must either (1) obtain a final decision "from a court of last resort" or (2) show that after 30 months of local proceedings, the investor is unable to obtain a final judgment. USMCA Article 14.D.5. Additionally, investors with general investments must serve the host state with a mandatory Notice of Intent to arbitrate the claims 90 days prior to filing the arbitration. USMCA Article 14.D.3. Accordingly, the investor may need approximately three years to comply with the requirements under the USMCA to be able to file the arbitration. The investor's assessment of these requirements and deadlines is critical as the investors' overall time limit to submit claims to arbitration under USMC is four years from the date the investor acquired, or should have acquired, knowledge of the treaty violation and the damages suffered.

Investors with covered investments do not need to exhaust local remedies before asserting a claim under the USMCA's investor-state dispute mechanism, but, like investors with general investments, they must wait for period of six months after the breach before submitting the dispute to arbitration to comply with the USMCA's cooling-off period and their claims are subject to a three-year time bar. USMCA Article 14.E.4.

USMCA Claims: Time Is of the Essence

For U.S. or Mexican investors who may have unfiled NAFTA legacy claims or new potential USMCA claims, it is necessary to consider options quickly given the deadlines and requirements under the USMCA outlined above. Quinn Emanuel has a specialized team of bilingual partners and associates who regularly conduct investment treaty cases in Spanish and English. We are always pleased to help assess if investors have a valid claim worth pursuing and if so, advise on the most favorable legal strategy for their claim.

Insurance Litigation Update

Insurance Coverage for Biometric Privacy Statute Suits: Recent Developments

In the last year, biometric privacy related litigation has been steadily increasing, and so have the insurance coverage disputed related to them. Illinois has been the center of this litigation in the last year due to its expansive Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA"), which was enacted in 2008. BIPA is intended to protect the privacy interests related to an individual's unique biometric identifiers such as fingerprints, facial geometry, and retina and iris scans and creates a private right of action for individuals to seek statutory liquidated damages. Since BIPA's enactments, additional states, such as California, New York and Massachusetts have introduced legislation based on BIPA.

The Illinois Supreme Court and district courts in Illinois have recently addressed claims brought pursuant to BIPA, including cases involving insurance coverage for those claims. These recent decisions will have broad implications for cases arising under BIPA and will contribute to the already robust volume of BIPA litigation, including the attendant coverage actions. To complicate matters more, on February 2, 2023, the Illinois Supreme Court unanimously held a five-year statute of limitations period applies to claims brought under all sections of BIPA. *Tims v. Black Horse Carriers, Inc.*, No. 2019-CH-03622, 2019 WL 13079191, at *2 (Ill. Cir. Ct. Sep. 23, 2019). And on March 16, 2023, an Illinois court granted class certification to a group of employees who alleged

their employer H&M violated their privacy by requiring them to scan their fingerprints to clock in and out while not properly collecting, storing or using the data pursuant to BIPA. *Slater v. H&M*, 2018 WL 6921177 (Ill. Cir. Ct. 2018). While this is certainly not the first instance in which a court has certified a class action with underlying BIPA claims, such decisions give BIPA plaintiffs momentum and disseminate a message that BIPA litigation is not slowing down. Indeed, on the same day as the decision in *H&M* was entered, Amazon became the first major corporation to be sued in a proposed class action lawsuit under New York City's Biometric Privacy Act.

These recent BIPA developments continue to expand potential liability for businesses, necessitating an understanding as to when and under what circumstances insurance may help cover the costs.

Policies That May Respond To BIPA Claims

Suits for violations of BIPA to date have mostly been brought by an employee of a company or as a class action on behalf of a class of employees. In most cases, companies should look to their commercial general liability ("CGL"), employment practices liability and cyber insurance policies for possible coverage. Insurers have raised several coverage defenses, most of which are based on policy exclusions, including, (1) the employment related practices exclusion, (2) the violation of statutes exclusion, and (3) the access or disclosure exclusion. The case law as to whether insurers must defend BIPA suits is mixed and depends on the policy language so insureds should carefully review their policies and press their insurers for coverage

Coverage Under CGL Policies

Courts have come to varying conclusions as to whether CGL policies cover BIPA claims. In 2022, the Supreme Court of Illinois found the insurer owed a defense under its CGL policy for a BIPA suit, holding the policy provided coverage for "personal injury." Specifically the court in *West Bend Mutual Insurance Company v. Krishna Schaumberg Tan, Inc.*, found the policy provided coverage and rejected the insurer's assertion the term "publication" in the covering provision requires "distribution" of "material that violates a person's right of privacy." The court explained the term "publication" is ambiguous as it can have more than one meaning—a "publication" can occur when where the information is shared only with one other party. Most recently, in *Continental v. Cheese Merchants*, the Northern District of Illinois found coverage was precluded based on several exclusions in the policy. In *Cheese Merchants*, an employee alleged the biometric time tracking system that used hand scans for authentication violated BIPA because the company purportedly gathered the biometric data without the employee's consent. The insurer sought declaratory judgment that it had no duty to defend the company under the policy based on (1) the "employment-related practices" exclusion; (2) the "disclosure of personal information" exclusion; and (3) the "violation of law" exclusion. The court held the employment-related practices exclusion does not preclude coverage because the requirement that employees clock in and out by scanning the backs of their hands did not come within the employment related practices intended to be excluded. However, the court held the other exclusions raised by the insurer were applicable and precluded coverage. With respect to the disclosure of personal information exclusion, the court reasoned the purpose of BIPA is to protect personal information and disagreed with the insured that the "disclosure of personal information" was not "health information" as one of the enumerated categories in the exclusion. The court explained, "health information" is similar, and likely even encompasses, "information about one's body (like the hand scans here)." The court also determined that the "violation of law" exclusion "sweeps broadly," finding that its broad nature encompassed plaintiff's claims under BIPA. *Id.* at *10. Contrary to the *Cheese Merchants* court, in *Thermoflex Waukegan LLC v. Mitsui Sumitomo Insurance USA Inc.*, the district court in Chicago ruled Mitusi had a duty to defend its insured for a BIPA suit under its umbrella policies. The court found the statutory violation exclusion is ambiguous and the data breach exclusion had to be construed in favor of coverage because it was limited to data breaches.

Practical Considerations

These recent decisions almost certainly will result in a significant increase in litigation, damages, and costs surrounding BIPA claims. With the increased use of biometric technology, private entities which collect and use biometric data should implement greater safeguards to ensure such data is transmitted only with the subject's consent. Further, ensuring robust privacy policies and data protection programs can help mitigate risk and ensure legal compliance. Any applicable policies should be closely reviewed for coverage, including CGL, employment practices liability insurance, and cyber insurance policies. Given that the bulk of coverage defenses are focused on exclusions, which must be narrowly construed in favor of coverage, insureds should press for coverage (unless and until insurers begin to specifically exclude BIPA claims). Insurers, on the other hand, should consider the risks and exposure associated with taking on clients that rely on biometric systems.

Cryptocurrency Litigation Update

Recent Legislative and Agency Efforts to Enhance Regulation of Digital Assets

The recent bankruptcies in the digital assets industry have prompted a renewed commitment among lawmakers and agencies to create a federal legislative and regulatory framework for digital assets. The industry currently faces both legal uncertainty and increased enforcement activity by the SEC, whose chairman, Gary Gensler, has asserted that most digital assets qualify as securities rather than commodities. Under consideration by Congress are two bills attempting to clarify the jurisdictions of the Commodities Futures Trading Commission ("CFTC") and the U.S. Securities and Exchange Commission ("SEC") over digital assets while enhancing consumer protections. Meanwhile, the Biden Administration has directed agencies to increase cross-agency cooperation and implement specific proposals to enhance federal oversight of the digital assets industry.

The bipartisan Responsible Financial Innovation Act (the "Lummis-Gillibrand Bill"), released in June 2022, proposed bright line rules for categorizing digital assets as commodities or securities. Notably, the Lummis-Gillibrand Bill proposes a narrower definition of digital assets as securities than under the traditional *Howey* test. Under *Howey*, assets qualify as securities when their purchases involve 1) an investment of money 2) in a common enterprise 3) with expectations of a profit 4) to be derived from the efforts of others. By contrast, under the Lummis-Gillibrand Bill, digital assets do not qualify as securities unless they grant purchasers rights in the business entity issuing the asset, such as a debt or equity interest, an entitlement to interest or dividend payments, or a share of the profit or revenue in that entity.

For digital assets that might be considered securities under the *Howey* test but not under this restrictive definition, the bill creates a novel class of "ancillary assets" as commodities. Ancillary assets are defined as digital assets, like Bitcoin and Ethereum, which are provided to purchasers under investment contracts but which do not grant purchasers rights in the business entities issuing the assets. In a move that has been criticized as favoring the digital assets sector, the Lummis-Gillibrand Bill grants exclusive jurisdiction over all non-security digital assets to the CFTC, an agency with a substantially smaller staff and enforcement budget as compared to the SEC.

At the same time, the Lummis-Gillibrand Bill would seek to enhance consumer protections by imposing disclosure requirements on ancillary asset issuers. Although less stringent than current securities disclosure requirements, these requirements impose 38 categories of issuer disclosures to be provided to the SEC semi-annually. The disclosure requirements apply if, over the preceding fiscal year, the daily average aggregate value of all trading in a given ancillary asset across the United States exceeded $5 million and the issuer, or a shareholder owning 10% or more of any class of equity shares in the issuer, engaged in entrepreneurial or managerial efforts that determined the value of the asset. The Lummis-Gillibrand bill thusly aims to enable consumers to make informed decisions with regard to the purchase of digital assets.

The Digital Commodities Consumer Protection Act (the "Stabenow-Boozman Bill"), made public in August 2022, assumes a similar approach to digital asset regulation albeit with less definitional clarity. Like the Lummis-Gillibrand Bill, the Stabenow-Boozman Bill provides a broad definition of digital commodities that includes cryptocurrencies such as Bitcoin and Ether, and grants the CFTC exclusive jurisdiction over digital commodities. However, in contrast to the Lummis-Gillibrand Bill, the Stabenow-Boozman Bill provides no guidance regarding whether digital assets qualify as securities. Accordingly, the passage of the Stabenow-Boozman Bill provides leverage to the SEC to continue to argue that many digital assets quality as securities.

The Stabenow-Boozman Bill arguably assumes a less robust approach to consumer protection than the Lummis-Gillibrand Bill. The only disclosure requirement for digital commodities in the Stabenow-Boozman Bill is registration with the CFTC. More specifically, rather than specifying required categories of disclosures for digital asset issuers, the Stabenow-Boozman Bill directs the CFTC to engage in rulemaking to develop disclosure requirements.

While Congress has delayed consideration of the Lummis-Gillibrand Bill and the Stabenow-Boozman Bill, the Biden Administration released a proposed framework for agency activity to address digital asset regulation. On March 9, 2022, President Biden released an Executive Order directing the U.S. Department of the Treasury ("Treasury") to work with other agencies to issue reports identifying financial stability risks, regulatory gaps, and policy recommendations.

Treasury subsequently published three reports in September 2022 outlining recommendations to enhance federal oversight over the digital assets sector. These recommendations included greater cross-agency coordination between among the U.S. Department of Justice, the SEC, and the CFTC to combat fraud and market manipulation involving digital assets; increased collaboration of interagency bodies such as the President's Working Group's Financial and Banking Information Infrastructure Committee, to identify and assess key risks related to digital assets, and an interagency working group, led by Treasury, that would consider the potential and

risks of adopting a U.S. Central Bank Digital Currency.

Based on Treasury's recommendations, on September 16, 2022, the White House released a report entitles "Comprehensive Framework for Responsible Development of Digital Assets." The framework directs agencies to implement a series of specific measures to enhance federal oversight of the digital assets industry. Notably, the framework calls on both the SEC and the CFTC to redouble their pursuits of enforcement actions. Among other directives, the framework tasks the Department of Commerce with establishing a standing forum to bring together federal agencies, business, academia, and the public at large to inform federal regulation of digital assets. In addition to identifying gaps in the United States' legal, regulatory, and supervisory regime governing over digital assets, Treasury is working to complete an illicit finance risk assessment on decentralized finance (DeFi) and will complete an assessment on non-fungible tokens (NFTs) by July 2023.

While the executive branch works to implement the September 2022 federal framework, legislators in both houses of Congress have called for additional legislation to address digital assets. In January 2023, House Republicans established the Subcommittee on Digital Assets, Financial Technology, and Inclusion. Overseen by the House Financial Services Committee, this subcommittee will work to provide regulatory clarity to the digital asset ecosystem. In particular, the subcommittee plans to construct a federal regulatory framework for stablecoins backed by the U.S. dollar.

More recently, in February 2023 the Senate Banking Committee held a hearing to discuss the recent crypto bankruptcies. The Committee heard testimony from law professors who shared varying proposals for digital asset regulation, ranging from a laissez-faire approach permitting industry self-regulation to an explicit grant of jurisdiction to the SEC as the primary enforcement of digital assets. During the hearing, Committee Chairman Sherrod Brown also proposed separating consumer funds from company assets, requiring clearer disclosures and transparency from digital assets issuers, and strengthening oversight and accountability. The Senate Banking Committee intends to develop new legislation related to digital assets over the coming year.

Numerous lawmakers have attempted to strike a balance between encouraging the growth of the digital assets sector and protecting consumers. Both the Lummis-Gillibrand Bill and the Stabenow-Boozman Bill err on the side of promoting industry growth by granting the CFTC, rather than the SEC, exclusive jurisdiction to regulate most digital assets. In contrast, the Biden Administration has called for greater cross-agency cooperation to establish a comprehensive regulatory framework for digital assets. These two approaches are, however, complementary in that both seek to provide greater clarity through legislation to pave the way for agencies to develop more specific expertise. Although Congress and the Biden Administration may not move in lockstep, the year ahead will certainly see a concerted effort by both branches of the federal government to establish a federal legal and regulatory framework for digital assets.

VICTORIES

Victory at the Federal Circuit

Quinn Emanuel achieved a significant victory for firm client C.R. Bard, Inc. when the Federal Circuit revived three patents, reversing the district court's summary judgment ruling in a case against competitor MedComp. The case ("Port 1") involves power injectable vascular access ports that are identifiable after implantation. It has been pending since January 2012, when Bard sued MedComp as well as AngioDynamics and Smiths Medical for patent infringement. The cases were stayed for seven years while the patents underwent reexamination.

While the cases were stayed, Bard, represented by another law firm, tried a case against Angio on patents directed to similar subject matter ("Port 2"). Judge Battalion, sitting by designation in the District of Delaware, granted JMOL and, *inter alia*, invalidated Bard's patents as patent ineligible under Section 101. Judge Battalion invoked the so-called "printed matter" doctrine and decided that because Bard's claims contain information—the message that the port is power injectable—they are patent ineligible under Section 101. Bard appealed and the Federal Circuit reversed, holding that Bard's claims are patent eligible as a matter of law. The Federal Circuit concluded that "although the asserted claims contain printed matter that is not functionally related to the remaining elements of the claims, each claim as a whole is patent eligible because none are solely directed to the printed matter."

Undeterred by the Federal Circuit holding in Port 2, MedComp alleged that Bard's Port 1 patents are invalid under Section 101 and moved for summary judgment. Bard argued in response, *inter alia*, that the Federal Circuit decision in Port 2 controls because the asserted claims are for Section 101 purposes the same as the Port 2

claims. Because the Port 2 claims are eligible as a matter of law, so too are the Port 1 claims. Chief Judge Shelby granted MedComp's motion and, although he recognized that his ruling "may appear in tension with the Federal Circuit's holding in" Port 2, he invalidated Bard's patents.

Bard appealed, and the Federal Circuit took just one week after oral argument to issue a decision in Bard's favor. The Federal Circuit agreed with Bard that Port 2 is "virtually identical to the [case] before us now." The Federal Circuit held that "[b]ecause we are bound by our precedent, we conclude that the asserted claims in Bard's three patents are directed to eligible subject matter under § 101." Now that Bard's patents have been revived, the three Port 1 cases, as well as two other cases involving similar patents, will proceed towards trial.

Landmark English Supreme Court Victory on Behalf of Ukraine

We are delighted to have assisted Ukraine in achieving its landmark victory in the Supreme Court in the claim brought by Law Debenture on behalf of the Russian Federation. The Judgment was handed down on 15 March 2023.

In one of the largest and most important cases to come before the English Courts in recent years, Law Debenture, instructed by Russia, first commenced proceedings against Ukraine in early 2016, and a team from Quinn Emanuel's London office led by partner Alex Gerbi was instructed to defend Ukraine. Law Debenture sought summary judgment, beginning an epic legal battle that came to cover a range of highly complex and uncertain areas of both domestic and international law, and lasted more than seven years, ending up with the recent seminal judgment of the Supreme Court.

In that Judgment, the Supreme Court held unanimously that Law Debenture is not entitled to summary judgment, with the result that there will be a full public trial before the English High Court of Ukraine's defence of duress resulting from Russia's alleged threatened use of force. The Supreme Court has held that Ukraine need show only that the alleged threats *"were a reason (not the reason, or the predominant reason, or the clinching reason)" for Ukraine's decision to enter into the contracts for the bonds, and that "[t]he onus will be on the Trustee to establish that those threats contributed nothing to Ukraine's decision".*

Further, the Court has made clear that *"[t]he alleged economic pressure, and threats of further economic pressure, are relevant as forming part of a combined strategy with the alleged threats of violence, or at least as part of the factual context in which those threats are alleged to have been made. If they accentuated the impact of the threats of violence, that is a factor which strengthens, not weakens, Ukraine's case".*

Whilst the Supreme Court explained that it had not been asked to consider events subsequent to the hearing of the appeal, which was concluded before Russia's invasion of Ukraine in February 2022, in his dissenting judgment, Lord Carnwarth, who would have allowed Ukraine's case to proceed to trial on broader grounds that the other Justices, said that those subsequent events cannot realistically be ignored.

Alex Gerbi, partner at Quinn Emanuel leading the case, comments: *"Ukraine greatly welcomes this opportunity to present its case on duress to the English Court on the merits, and to have a full public and impartial judicial consideration of that case, with the requirement for full disclosure by Russia in respect of its conduct towards Ukraine."*

This Judgment has received legal industry and public attention around the world, and has opened up the next chapter in this battle between the two sovereign states as the case moves back to the English High Court, Financial List, for a full public trial. It is certain to be one of the most keenly watched cases internationally over the coming years.

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 April 2023, 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
BEIJING
BERLIN
BOSTON
BRUSSELS
CHICAGO
DALLAS
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