

00000



Rx For The Defense

5/8/2019 Volume 27, Issue 2

Looking for **Targeted Contacts?**



Hit the Bullseye with Cri

Contact Laurie Mokry at Imokry@dri.org or 312.698.6259

Committee Leadership



Chair Sara J. Gourley Sidley Austin LLP Chicago, IL



Vice Chair
Gail Rodgers
DLA Piper LLP (US)
New York, NY

Editors



Kimberly L. Beck Ulmer & Berne LLP Cincinnati, OH



Heather M. Howard King & Spalding LLP Atlanta, GA

Click here to view entire Leadership

www.mrchouston.com (888)868 - 6769Established 1983 Legal Nurse Record Retrieval Medical Subpoena Research Chronologies & **Data Mining** Summaries HIPAA & HITECH Utilization Review Secure Database Personal Injury Cost Estimator Review Order Online RECORDS BASED

In This Issue

Leadership Notes

From the Chair......2

By Sara Gourley

From the Editors......2

Feature Articles

"How Safe Is Your Data? Emerging Liability Concerns with Maintaining Medical App and Smart Device User Data"...... 4 By Russell J. Chibe

Government Action SLG

Legal Drug Manufacturers as Illegal Drug Dealers: The Recent Attempt to Use the Drug Dealer Liability Act in Tennessee to Recover Directly from Opioid Manufacturers 6 By Jeffrey E. Nicoson

Leadership Notes

From the Chair

By Sara Gourley



Our 2019 seminar is right around the corner, but there is still time to register. We will gather at the Renaissance Hotel Downtown in Washington, D.C. By now you should have received your brochure and other notices about the

exciting program our planning committee has in store.

This year's seminar will feature more opportunities to network with clients and colleagues, including dinearounds at dinner before the conference, at lunch during the conference, and social events sponsored by DRI and by participating law firms. As always, there will be topnotch presentations on a variety of topics, including how to conduct a successful cross-examination of plaintiff's expert witnesses, conceptualizing the attitudes of jurors in a politically polarized climate, and ways to address FDA evidence in medical device cases. In addition, we will have our annual Young Lawyers Blockbuster, and an exclusive In-House Counsel Only Breakout. The seminar will close with our annual service project. Please join the DRI community in supporting the Community for Creative Non-Violence, a shelter serving the homeless in D.C. A short walk from the conference site, you will end your stay having worked alongside clients and colleagues to make a difference!

In addition to our wonderful CLE program, numerous companies will hold counsel meetings in connection with our seminar, so watch for invitations to those from your clients. If you and your colleagues have not yet done so, please register immediately and book a room at the Renaissance Washington D.C. Downtown Hotel. When you register, you will also have the opportunity to sign up for the Supreme Court tour (limited space, participants will be selected by lottery). We always have a great time, and you will not want to miss out.

As a bonus, if you register for the May 16–17 Drug and Medical Device Seminar, you can also attend the Cannabis Law Seminar on May 15 for just \$190!

I look forward to seeing you in Washington, D.C.

Sara Gourley is a partner in the Chicago office of Sidley Austin and a practice leader for the Firm's Product Liability and Mass Tort practice. She focuses on the national and regional defense of drug and medical device litigation. She is Chair of the Drug & Medical Device Committee of DRI.

From the Editors





If you are interested in writing an article for publication in RX for the Defense please contact Kim Beck at kbeck@ulmer.com or Heather Howard at hhoward@kslaw.com

to find out more information about the publication guidelines and the selection process.

Kimberly Beck practices in the Cincinnati, Ohio office of Ulmer & Berne LLP, where she is a member of the firm's Pharmaceutical and Medical Device Defense and Mass Tort practice groups. Her practice focuses on the defense of pharmaceutical products. Kimberly currently serves as the Chair of Counsel Meetings and Newsletter Editor for the DRI Drug and Medical Device Committee as well as the Treatise Chair and Networking Vice Chair for the Product Liability Committee.

Heather Howard is Counsel in the Atlanta office of King & Spalding LLP, where she is a member of the firm's Trial & Global Disputes practice. Ms. Howard focuses her practice on the defense of pharmaceutical and device manufacturers in product liability suits at the trial level and on appeal. Heather serves as the Assistant Newsletter Editor for the DRI Drug and Medical Device Committee.

Feature Articles

Component Preemption After Shuker v. Smith & Nephew, PLC

By David J. Walz



In Shuker v. Smith & Nephew, PLC, 885 F.3d 760, 768 (3d Cir. 2018), the Third Circuit Court of Appeals addressed an issue of first impression in the appellate courts. The issue was how to "apply the Medical Device Amendments"

express preemption provision to a 'hybrid system,' i.e., a system that is itself a 'device' but that is comprised of Class Il components in addition to one or more Class III components." Id. In other words, the court addressed express preemption's application under Riegel v. Medtronic, Inc., 552 U.S. 312 (2008), when some of the components implanted in the plaintiff underwent premarket approval while others did not. The issue is important because surgeons are free to engage in off-label use of components, including the use within the same medical procedure of components with different regulatory backgrounds. A negative preemption decision in Shuker would have raised the risk that medical-device manufacturers could face liability under state law depending not upon whether they complied with federal rules and regulations, but the surgeon's decision to use various components.

In *Shuker*, the plaintiffs urged the court to conclude "that the 'device' at issue is the entire hybrid system itself" and that PMA preemption did not apply "when a component is used off-label in a manner 'that was never studied or approved by the FDA'" and the "component part was pre-approved for use with another system." 885 F.3d at 772 (quoting the plaintiffs' brief).

The Third Circuit rejected that approach and reached the proper conclusion that preemption applies at the component level so that a PMA component may retain the protections afforded by preemption even when used with non-PMA components.

The court agreed with the manufacturer's arguments and the FDA's amicus brief and held that the specific component with which the plaintiff takes issue is the proper focus of the preemption analysis. The court provided three specific reasons for its holding. First, applying the "analysis at the component level finds support in the text of the statute and regulations." *Id.* "The Federal Food, Drug, and Cosmetic Act ["FDCA"] defines 'device'" to "include[] 'components, parts, and accessories." *Id.* (citing 21 U.S.C. \$321(g), (h)). Therefore, this definition, coupled with the

fact that neither it nor 21 U.S.C. §360k(a) "makes any exception for instances where components that received premarket approval are used with components that did not receive such approval," supported the component-focused approach. *Id.* at 772 n.10.

Second, the FDCA's allowance of "off-label use supports a component-level analysis." *Id.* at 772. The FDCA "contemplates that physicians will prescribe or administer components outside of a system with which the FDA approved their use" and "the regulatory landscape contemplates that devices may be broken down into component parts and individual components used separately by third parties." *Id.* at 773. Under this regulatory scheme, the manufacturer complies with federal law through the premarket-approval process and does not become subject to state-law liability "when a single component of a Class III device is used on its own, rather than in the premarket-approved system." *Id.*

Third, the FDA takes the position that "the relevant device for preemption purposes must be evaluated at the component level." *Id.* Indeed, FDA is charged with "establish[ing] performance standards for device *components*... 'where necessary to provide reasonable assurance of ... safe and effective performance." *Id.* (quoting 21 U.S.C. \$360d(a)(2)B)(i)) (emphasis added).

Thus, the court held the following:

Taken together, the statutory definition of "device," the treatment of off-label uses, and the guidance of the FDA all counsel in favor of scrutinizing hybrid systems at the component-level. . . . And the *Riegel* test is properly framed at Step One as "whether the Federal Government has established requirements applicable" to a component of the hybrid system.

Id. at 774. Because the "heart" of the plaintiff's claims alleged defects in the PMA component, the claims "challenged the safety and effectiveness of [the PMA component]" and were preempted. Id.

In reaching this holding, the court discounted the reasoning of the handful of trial courts that had refused to apply express preemption to "complaints that allege 'injuries stemming from the combination of [premarket and non-premarket] component parts." *Id.* at 775 n.14 (citing cases). Instead, the court aligned itself with the trial

courts that had reasoned similarly and held such claims preempted. *Id.* at 774 n.12 (citing cases).

The holding in *Shuker* is important for several reasons. Adoption of the plaintiffs' argument that preemption simply disappears whenever a non-PMA component is used would have negatively impacted manufacturers' views on off-label use. Indeed, the Shuker court recognized this point, reasoning that "Congress thereby has evinced an intent not to 'discourage[]' device manufacturers 'from seeking . . . approval of devices with potentially beneficial off-label uses for fear that such use might expose the manufacturer . . . to unpredictable civil liability." Id. at 773 (quoting Buckman Co. v. Plaintiffs' Legal Comm., 531 U.S. 341, 350 (2001)). On a related note, undermining express preemption for some components based on some uses would inject uncertainty and unpredictability into a manufacturer's risk assessment. Finally, determining the preemptive protection afforded to a component based not on its regulatory approval, but to its use as a matter of medical judgment, is poor policy on both the healthcare and liability fronts.

In the end, the result in *Shuker* serves to deter an endrun around *Riegel* and an unnecessary expansion of litigation and potential liability. As the only appellate court to have weighed the issue, and having done so with the aid of FDA's explanation of its position, *Shuker* should deter other plaintiffs' counsel from pursuing the "hybrid system" theory of liability to defeat preemption. To that end, although various cases in the federal trial courts had attempted to use that theory to make inroads against preemption in the years before *Shuker*, no court has cited or applied *Shuker* on this specific point in the year since it was issued. Overall, the Third Circuit's well-reasoned opinion should provide the starting and stopping points for other courts' analysis in future years.

David J. Walz is a shareholder in the Tampa office of Carlton Fields, P.A. Dave focuses on the defense of actions involving all types of prescription medicines, medical devices, and over-the-counter medical products. He is a member of the DRI Drug and Medical Device Steering Committee, Product Liability Committee, and Litigation Skills Committee, along with various other professional and defense organizations.

"How Safe Is Your Data? Emerging Liability Concerns with Maintaining Medical App and Smart Device User Data"

By Russell J. Chibe



In February of 2019, cloud access security broker Bitglass published its annual Healthcare Breach Report, finding that hacking and IT incidents were the greatest threat to health information security in 2018. The next month,

the Food and Drug Administration ("FDA") announced its first cybersecurity safety communication of 2019, warning of vulnerabilities in the wireless telemetry technology of an implantable cardiac device. For those of us who represent pharmaceutical and medical device companies, the risk of lawsuits alleging injuries from defective products is an omnipresent concern. However, if you or your client is developing a mobile medical app or smart medical device, the liability involved in handling client data—liability which often does not require any specific injury or harm—is becoming an increasing concern.

Managing client data, including private health information, can be particularly challenging for device manufactur-

ers and app developers because multiple regulatory bodies may have guidelines or rules to consider. The Federal Trade Commission ("FTC") can take action on behalf of consumers where it believes a manufacturer is mishandling customer data. The FDA considers cybersecurity in its premarket approval process and will issue statements regarding security threats. The U.S. Department of Health and Human Services Office for Civil Rights ("OCR") also has the power to enforce the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") where applicable. And of course, the threat of civil litigation—be it an individual plaintiff or a class action—is always looming.

Manufacturers of smart devices, medical or not, face the risk of both Federal Trade Commission actions and private lawsuits when they fail to properly protect user data. The FTC will commence an action against a company pursuant to Section 13(b) of the Federal Trade Commission Act where it has "reason to believe" that the law has been violated and that taking action against the company is in the public interest. Generally, with respect to the Internet of Things, these complaints allege "unfair or deceptive acts" based on both the promises of the manufacturer and the reasonable expectation of the consumer.

The good news for manufacturers and developers is that the FTC has sought to increase its transparency regarding what it believes is reasonable data security. For example, in January of 2015, the FTC published *Internet of Things: Privacy & Security in a Connected World.* In June of the same year, it published *Start with Security: A Guide for Business.* This publication examines multiple FTC investigations and offers guidance regarding best practices for data maintenance. Further, in July of 2017 the FTC launched a blog entitled "Stick with Security," which picked up where *Start with Security* left off. The "Stick with Security" blog specifically notes that one common thread in investigations that are closed without charges is that companies followed the guidelines established in *Start with Security.*

The best practices for data security outlined by the FTC effectively establish a reasonableness standard by which developers may be judged should the Commission launch an investigation. Topics addressed include who should have access to data, the appropriate levels of security when storing and transmitting data, and procedures for addressing vulnerabilities that may arise. Most actions undertaken by the FTC with respect to smart devices allege that manufacturers failed to take appropriate steps to address well-known and easily preventable security flaws, so it is critical that developers have procedures in place for monitoring possible security risks.

The FDA offers additional cybersecurity guidelines for device manufacturers. In 2013 it established a Cybersecurity Working Group which subsequently issued premarket and postmarket guidance for device manufacturers in 2014. More recently, it published a *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*, which outlines a framework for preparing for and responding to cybersecurity incidents around medical devices. The FDA does not have the enforcement power of the FTC, but it does consider cybersecurity as part of its premarket approval procedure. Adhering to the FDA's guidance will not only ensure that a device makes it to market, but it can be further evidence that the manufacturer has taken proper steps to secure its device, including the data it may transmit, should regulatory action or a lawsuit commence.

Beyond the FTC and the FDA, the risk of private lawsuits for data breaches remains a concern—particularly where

data is sensitive. Last year a settlement involving a "smart" sex toy grabbed headlines given its salacious subject matter, but the case is instructive for manufacturers of smart medical apps. In *N.P. v. Standard Innovation (US) Corp.*, Case No. 1:16-cv-08655 (N.D. III.), after the manufacturer's database was compromised in front of a live audience at a hacker conference, a class action lawsuit quickly followed and the company eventually settled for \$3.75 million. Two primary factors drove such a large settlement: the fact that the defendant had alleged that user data was not being stored on its server when it actually was, and the fact that the data at issue was highly sensitive.

Outside of smart devices and apps, lawsuits involving healthcare data breaches provide further insight as to the potential risk should a hacker gain access to patient data through a smart medical device or app. In 2014, two class action lawsuits—*Curry v. AVMed, Inc.*, Case No. 1:10-cv-24513 (S.D. Fla.) and *Springer v. Stanford Hospitals*, Case No. BC470522 (Cal. Sup. Ct.)—alleging that protected health information was lost, stolen or inappropriately accessed were settled in Florida and California for \$3 million and \$4.125 million, respectively. Both of these cases were settled despite a lack of evidence that the data was used to any plaintiff's detriment.

In addition to private lawsuits, any device handling protected health information is subject to the provisions of HIPAA, which means that OCR can also bring enforcement actions against app and device developers should HIPAA's provisions be violated. Thankfully, in the same way that the FTC has offered guidance for compliance, the OCR has published "Health App Use Scenarios & HIPAA," a document available on their website that outlines best practices to ensure compliance with HIPAA. Most important for developers is determining whether they are either a covered entity (*i.e.*, health plans, health care clearinghouses and most health care providers) or a business associate of a covered entity. If the app or device was not created at a health care provider's instruction, there is a high likelihood that HIPAA does not apply.

Perhaps the biggest takeaway for medical device and app manufacturers is that, unlike hacks that result in product malfunctions, a company can find itself liable for data breaches even where no clear harm has resulted. With this in mind, it is important that companies familiarize themselves with FDA, FTC and OCR guidance from the earliest stages of the product's development. Indeed, many manufacturers find it valuable to have a specific cybersecurity officer; it is important that they focus not only on potential malfunctions but also on data security.



Beyond the design of the device itself, private health information security should be a focus with respect to database management and customer terms and conditions as well. To limit liability, companies should be very careful about who has access to user data, and always make sure to be very transparent—and seek permission when necessary—when collecting customer information. Whether it is a government agency or a plaintiff's lawyer calling, companies want to be able to show that data security was

a concern from drawing board to marketplace, and that they took every appropriate step along the way.

Russell J. Chibe is a senior attorney at Drinker Biddle & Reath, LLP, where he works on state and federal complex litigation matters at both the trial and appellate phases and has significant experience with multidistrict litigation on behalf of major pharmaceutical companies. In addition to defending manufacturers of medical devices and medications, Russ also assists product manufacturers and app developers in a variety of areas including labeling and regulatory compliance.

Government Action SLG

Legal Drug Manufacturers as Illegal Drug Dealers: The Recent Attempt to Use the Drug Dealer Liability Act in Tennessee to Recover Directly from Opioid Manufacturers



By Jeffrey E. Nicoson

The misuse and abuse of opioid medication is a prevalent topic in the public realm. The National Institutes of Health ("NIH") has concluded that "opioid misuse and addiction" is a

"public health crisis." U.S. Dep't of Health & Human Servs., Nat'l Institutes of Health, <u>HEAL Initiative Research Plan</u> (last accessed Mar. 24, 2019). NIH reports that, as of 2017, "[m]ore than 2 million Americans have opioid use disorder (OUD), and millions more misuse opioids, using them for durations, doses, or reasons other than prescribed," which has "resulted in an alarming increase in opioid addiction and overdose deaths." *Id.* NIH also believes these numbers may be underestimated. *See id.*

Opioid use and prescription statistics in the State of Tennessee are emblematic of the concerns NIH raises. In 2015, medical providers in Tennessee issued more than 7.8 million prescriptions for opioid pain medication. See National Institute on Drug Abuse, Tennessee Opioid Summary (last accessed Mar. 24, 2019). That number of prescriptions equals a rate of 118.3 prescriptions per 100 persons in Tennessee. See id. It exceeded the national average of 70 prescriptions per 100 persons. Id. In 2016, 1,186 persons died in Tennessee due to opioid-related overdoses. Id. This, too, exceeded the national average. Id.

Lawsuits have long been used to try and saddle drug manufacturers with monetary damages related to misuse and abuse of prescription medications. Manufacturers are an obvious litigation target given that the drugs are their drugs and they have the deepest pockets. Legal theories asserted against drug manufacturers range from general theories of negligence to products liability theories to civil conspiracy claims to violations of state consumer protection laws. See Richard Ausness, The Role of Litigation in the Fight Against Prescription Drug Abuse, 116 W.Va. L. Rev. 1117 (2014).

Drug manufacturers have largely been successful in fending off those causes of action on causation grounds. *See id.* at 1163. As an example, Purdue Pharma, the maker of OxyContin, "has been able to shift much of the blame to 'pill doctors' who have prescribed OxyContin in excessive quantities to their patients, arguing that their prescribing practices broke the chain of causation." *Id.*

Recent litigation in Tennessee has seen a new approach seeking to outflank the causation problem that arises when someone else illegally distributes an opioid manufacturer's mediation. Recent lawsuits filed in eastern Tennessee seek to hold opioid manufacturers liable under the Tennessee Drug Dealer Liability Act ("DDLA"), Tenn. Code Ann. §29-



38-101 *et seq* (full disclosure: the author's firm is involved in these cases).

Statutes like the DDLA are recent developments in state statutory law. See Validity, Construction, and Application of State Drug Dealer Liability Acts, 12 A.L.R.7th Art. 2 §2 (2019). "In 1992, a former United States Attorney proposed legislation that would provide third-party plaintiffs with a civil remedy for injuries caused by the use of illegal drugs." Id. That proposal led to a comprehensive Model Act being drafted. See Daniel Bent, The Model Drug Dealer Liability Act (last accessed Mar. 24, 2019). The Model Act's "market liability" language "provides for civil liability for any drug dealer in a community for the injuries to others by drug users of the same type of drug, during the time period the dealer was dealing in the same community." Id. "Under 'market liability' a plaintiff need not prove that the particular defendant drug dealer was in the 'chain of distribution' to the user that caused the injuries" in order to recover. Id. Seventeen states have now enacted their own drug dealer liability statutes. See id.

Tennessee enacted its DDLA in 2005 as a "civil remedy for damages to persons in a community injured as a result of illegal drug use" so "injured persons [can] recover damages from those persons in the community who have joined the illegal drug market." Tenn. Code Ann. §29-38-102. The DDLA "shift[s], to the extent possible, the cost of the damage caused by the existence of the illegal drug market in a community to those who profit from that market." Id. The statute is intended to address prior case law holdings where "only those dealers in the actual chain of distribution to a particular user could be sued." Id. §29-38-103(7). Tennessee has not fully adopted the market liability theory as that theory "has been shown to be destructive of market initiative and product development when applied to legitimate markets." Id. §29-38-103(9). Instead, it "expressly adopts a legislatively crafted form of liability for those who intentionally join the illegal drug market." Id.

The DDLA allows a litigant to recover monetary damages against "[a] person who knowingly participates in the illegal drug market within [the state of Tennessee]." *Id.* §29-38-105(a). An "illegal drug market" is defined as the "support system of illegal drug related operations, from production to retail sales, through which an illegal drug reaches the user." *Id.* §29-38-104(2). Participation in the illegal drug market centers on actual distribution, possession with intention to distribute, acting to facilitate distribution, or an agreement to accomplish one of those outcomes. *Id.* §29-28-104(9). The only exclusion is for law enforcement officers, or persons working with law

enforcement officers, who are selling drugs in the illegal market "if the participation is in furtherance of an official investigation." *Id.* \$29-38-105(b).

The initial Tennessee DDLA lawsuit was filed in Sullivan County in June of 2017. *Barry Staubus, et al. v. Purdue Pharma, L.P., et al.*, Case No. C-41916 (Sullivan County Cir. Ct.). The second lawsuit was filed in Campbell County in September of 2017. *Jared Effler, et al. v. Purdue Pharma, L.P., et al.*, Case No. 16596 (Campbell County Cir. Ct.). A third matter was filed in Cumberland County in January of 2018. *Bryant C. Dunaway, et al. v. Purdue Pharma, L.P., et al.*, Case No. CCI-2018-CV-6347 (Cumberland County Cir. Ct.).

The plaintiffs are District Attorneys General of various eastern Tennessee counties along with various victims, or representatives of victims, of purported illegal drug markets. The lawsuits name several manufacturers of opioids, chiefly Purdue Pharma, Mallinckrodt LLC ("Mallinckrodt"), Teva Pharmaceuticals ("Teva"), and Endo Health Solutions ("Endo"). The lawsuits also name medical practices that are alleged "pill mills" and convicted drug dealers who supplied drugs illegally.

The plaintiffs, however, are focused on Purdue Pharma, Mallinckrodt, Teva, and Endo. Their primary legal theory asserts, generally, that the "pharmaceutical defendants supplied and materially supported the illegal drug market through the production and dissemination of massive quantities of prescription opioids, all while knowing about (but failing to address) downstream diversion into illicit channels by unscrupulous doctors, pill mills, and drug dealers." Joe P. Leniski, Jr., Taking A Drug Epidemic To Court: Tennessee's Drug Dealer Liability Act (DDLA) (last accessed Mar. 24, 2019.) The lawsuits also discuss, in detail, supposed "fraudulent and deceptive marketing campaigns intended to influence the medical community and increase the sale of [] opioid medications." Order Granting Mfg. Defs.' Mot. To Dismiss ¶ 3, Jared Effler, et al. v. Purdue Pharma, L.P., et al, Case No. 16596 (Campbell County Cir. Ct. Oct. 5, 2018) (the "Campbell County Order"). These campaigns occurred even though Purdue Pharma, Mallinckrodt, Teva, and Endo "knew their opioid medications were addictive and being abused[.]" Id. Those manufacturers allegedly participated in the illegal drug market because "they knowingly condoned, encouraged, failed to prevent, and capitalized upon this knowledge by selling more opioid tablets than could be appropriately prescribed by doctors." Id.

The plaintiffs also rely on definitional language in the DDLA that defines a "person" to include a corporation,

Tenn. Code Ann. §29-38-104(11), and the broad definition of an "illegal drug market" to include conduct "from production to retail sales," *id.* §29-38-104(2). Coupling that language with the DDLA's purpose "to shift . . . the cost of the damage caused by the existence of the illegal drug market in a community to those who profit from that market," *id.* §29-38-102, the plaintiffs take the position that opioid manufacturers fall within the DDLA because they are participants in the chain of distribution with foreseeable knowledge that their drugs were being illegally distributed or overprescribed.

Purdue Pharma, Mallinckrodt, Teva, and Endo have sought dismissal of these lawsuits and challenged the assertions that the DDLA applies to them. See, e.g., Mot. to Dismiss 3d Am. Compl, Jared Effler, et al. v. Purdue Pharma, L.P., et al., Case No. 16596 (Campbell County Cir. Ct. July 27, 2018). They pointed out that the plaintiffs were attempting to equate them with street-level, illegal drug dealers when all of their opioid mediations are lawfully manufactured and approved by the Food and Drug Administration ("FDA") for distribution. See id. They also argued that the FDA-approved opioid mediations were lawfully sold within Tennessee laws and regulations to medical practices that were registered with the Drug Enforcement Agency ("DEA"). See id. Finally, they argued that the plain language of the DDLA does not intend to cover them for the lawful sales of opioid medication that are then illegally sold on a secondary market. See id.

These motions have had mixed results. In October 2018, the court in Campbell County granted the motion to dismiss and dismissed Purdue Pharma, Mallinckrodt, Teva, and Endo. See Campbell County Order. That court concluded there was no viable cause of action since opioid manufacturers "that manufacture FDA-approved opioid medications and sell to DEA-licensed distributors are not 'drug dealers' as contemplated by the DDLA" and "the

DDLA does not apply to manufacturers who are legally producing and distributing opioid medication." Id. ¶ 11. That decision is now on appeal before the Tennessee Court of Appeals.

In contrast, the court in Sullivan County denied a motion to dismiss by Purdue Pharma, Mallinckrodt, Teva, and Endo. The order did not go into as much detail as the dismissal order from Campbell County. Purdue Pharma, Mallinckrodt, Teva, and Endo, after being denied a request for interlocutory appeal, then asked the Tennessee Court of Appeals to grant them an extraordinary appeal and to stay proceedings in Sullivan County pending resolution of the Campbell County case. The Court of Appeals denied this request without prejudice on the ground that there was no sufficient basis for granting an extraordinary appeal.

The outcomes of these cases are far from settled as the Tennessee Court of Appeals will eventually rule on whether the DDLA can apply to FDA-approved opioid manufacturers who lawfully distributed their medications even though others then subsequently illegally resold or redistributed those same medications. Given causation has been a critical element in prior tort law efforts to obtain compensation from opioid drug manufacturers, these cases should be watched closely to see what the ultimate outcome is and how it could impact pharmaceutical manufacturers in the states where similar DDLAs are in force.

Jeffrey E. Nicoson is a member in the Memphis office of Leitner, Williams, Dooley & Napolitan, PLLC. Mr. Nicoson's practice focuses on the defense of product liability, personal injury, healthcare liability, commercial litigation, and governmental tort liability lawsuits. He is a member and participant in the DRI Drug & Medical Device Defense of Government Actions specialized litigation group.