



SWANSON, MARTIN & BELL, LLP

**Post-Pandemic Litigation -
What to Expect**

April 21, 2021

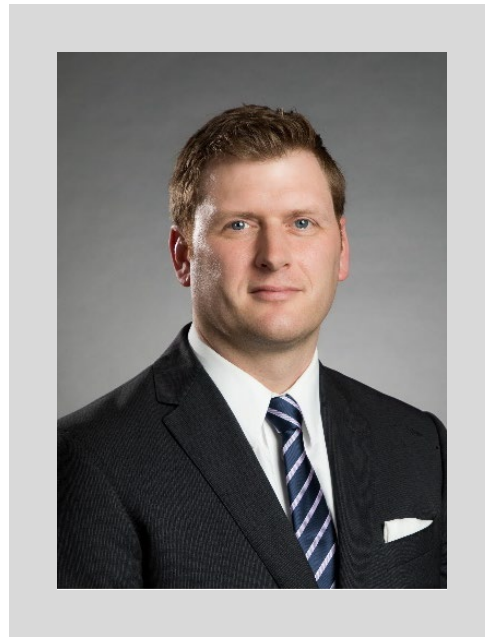
**John P. Arranz
Robert W. Stephens
Marcie J. Vantine**

Attorneys, Swanson, Martin & Bell, LLP

Swanson, Martin & Bell, LLP Presenters:



John P. Arranz



Robert W. Stephens



About Swanson, Martin & Bell, LLP

- Founded in 1992 by 13 attorneys, who, at the time of their departure, represented the core of the defense trial practice at a large Chicago law firm.
- Founded on the principles of providing high-quality and cost-effective legal representation to corporate and insurance clients.
- SMB today:
 - More than 130 lawyers;
 - 30 practice areas;
 - Four Illinois offices (Chicago, Libertyville, Lisle, Edwardsville) and offices in Hammond, Indiana and St. Louis, Missouri.
- Fortune 500 and large corporations routinely hire SMB for work on a national basis.

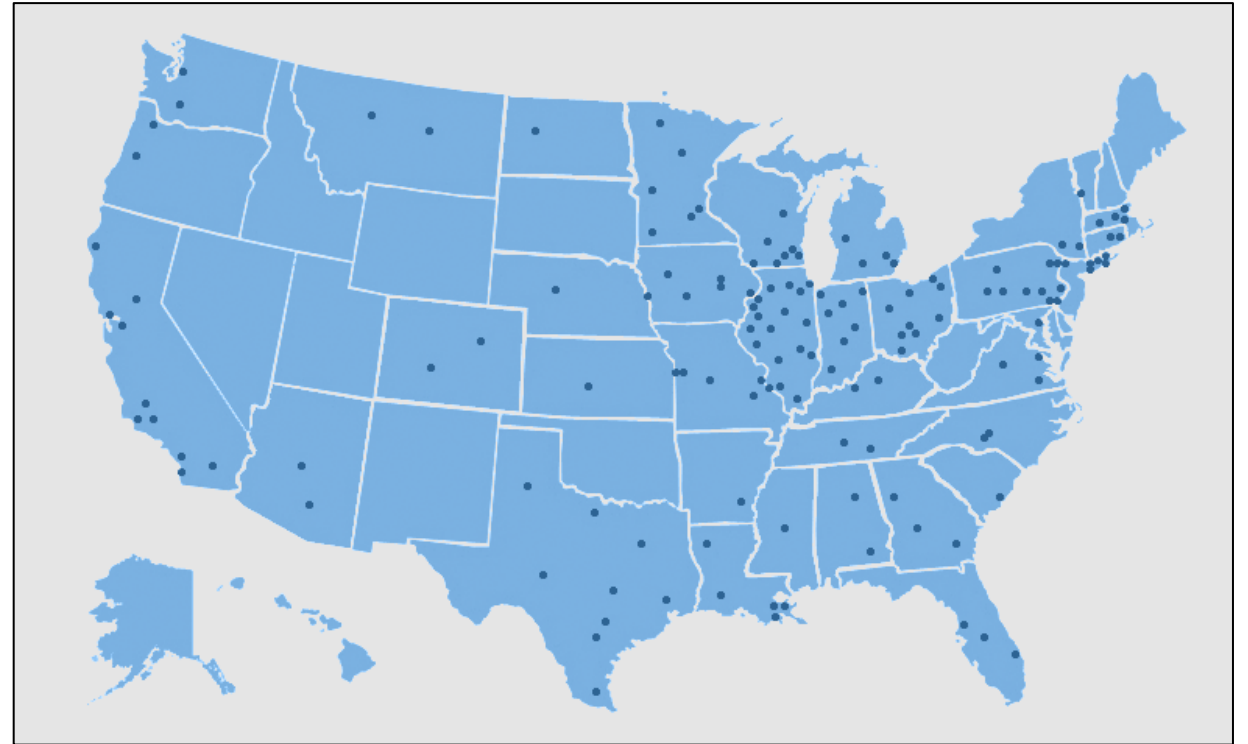


Practice Areas

- Admiralty, Maritime & Transportation
- Appellate Practice
- Asbestos & Toxic Tort Litigation
- Aviation Litigation
- Cannabis Law
- Civil Rights and Governmental Liability
- Class Action Defense
- Commercial Litigation & Business Disputes
- Construction
- Creditors' Rights & Bankruptcy
- Data Protections & Information Privacy
- Employment Litigation & Counseling
- Entertainment & Media Law
- Equipment Leasing
- Family Law
- Fidelity & Surety Bond Claims
- Fire & Explosion Litigation
- General Trial Practice
- Insurance Defense
- Intellectual Property Litigation & Transactional Services
- Lawyers Liability
- Mediation Practice
- Medical Negligence & Healthcare
- Occupational Safety & Health (OSHA)
- Pharmaceutical & Medical Device
- Product Liability
- Professional Liability
- Professional Licensing
- Real Estate Litigation & Transactional Services
- Wills, Trusts & Estates

Trial Experience and Map

- Litigation is SMB's hallmark.
- SMB lawyers have:
 - Tried over 1,000 cases to verdict;
 - Appeared or managed litigation in almost every major venue in the United States;
 - Tried cases to verdict in 35 states (blue dots).



Reopening of Area Courts

- **St. Louis City, Missouri Circuit Court**
 - Presiding Judge Michael F. Stelzer has announced that as of April 7, 2021, jury duty schedule has resumed as normal.
 - St. Louis City is in Phase Two of the reopening set forth by the Missouri Supreme Court.
 - Judge Stelzer anticipates the civil trial docket will resume by the end of 2021.
 - Criminal trials will take precedent based on a defendant's constitutional right to a speedy trial.



Reopening of Area Courts

- **St. Louis County, Missouri Circuit Court**
 - Presiding Judge Michael Burton issued an Order dated April 9, 2021, which addressed the current status infection rates, vaccine rates, and opinions of public health experts.
 - St. Louis County is in Phase Two of the reopening set forth by the Missouri Supreme Court. Access to the courthouse is still limited.
 - St. Louis County resumed limited in-person jury trials in criminal cases only on April 12, 2021.
 - According to Judge Burton, it will be “some time” before civil cases will be able to be tried.



Reopening of Area Courts

• **Madison County, Illinois Circuit Court**

- Chief Judge William Mudge issued an Order effective March 1, 2021, regarding the limited reopening of Madison County, Illinois courts.
- Pursuant to this Order, no civil jury trials shall be conducted until further order of the assigned judge after consultation with the Chief Judge to determine if the trial can proceed safely.
- Non-jury trials, both in person and via videoconference, may be scheduled at the direction of the assigned judge on a case by case basis.
- All motions and case management conferences shall be conducted remotely via telephone or videoconferencing, unless the assigned judge allows the motion to be heard in person in accordance with social distancing and protective equipment.
- In an February 11, 2021 Order from the Madison County, Illinois Circuit Court Civil Division the Court set forth the process for rescheduling trial dates.



Reopening of Area Courts

- **St. Clair County, Illinois Circuit Court**
 - Presiding Judge Andrew Gleeson issued an Order effective March 1, 2021, regarding the limited reopening of St. Clair County, Illinois courts.
 - Pursuant to this Order, all civil jury trials currently scheduled in 2021 are to be reset on a case by case basis.
 - St. Clair County is continuing to encourage the use of remote proceedings for all non-emergent matters.
 - St. Clair County has published “Guidelines for Virtual Courtroom Proceedings of the Twentieth Judicial Circuit.”



Poll Question #1:

- **When employees at your company return to work, will they:**
 - A) Return to the office full time.
 - B) Continue to work from home.
 - C) Hybrid (in office some days and from home some days).
 - D) Depends on the employees job duties.



Litigation Arising from the Pandemic

• Force Majeure

- When a company declares “force majeure,” it is invoking a clause, typically noted in its contract with its clients, that states that due to circumstances beyond its control, it is unable to fulfill the terms of the contract.
- If no force majeure clause in contract, must rely on non-contractual common law doctrines (impossibility and frustration of purpose) in order to excuse non-performance under a contract.
- Missouri has no statutory definition of force majeure, so must rely on case law.
- Illinois has no statutory definition of force majeure.
 - Illinois courts have relied on Black’s Law Dictionary definition of force majeure.



Litigation Arising from the Pandemic

- **Medical Malpractice Litigation**
 - Failure to Diagnose
 - Failure to Adequately Treat
 - Failure to Protect Against Virus Spread
- **Occupational Safety & Health Administration (OSHA)**
 - Imposition of penalties on employers for:
 - Alleged failures to provide personal protective equipment (PPE) and other workplace safety measures;
 - Violations of employees exposures; and
 - Hospitalization reporting requirements.
 - Employers defending OSHA violations.
 - Retaliation claims filed by employees based on reporting alleged OSHA violations.



Legislation Arising from the Pandemic

- **Missouri Senate Bill 51**
 - Limits Civil Actions for:
 - Exposures to COVID-19
 - COVID-19 Medical Liability Action
 - COVID-19 Products Liability Action
 - Currently with the House Committee on Rules - Legislation Oversight.
 - If passed will go into effect on August 28, 2021.
 - Contains an expiration date – would expire four years after effective date of act.



Executive Orders Arising from the Pandemic

- Provides certain protections – especially to health care providers.
- Limits liability in the event that the provider canceled elective procedures.
- Limits liability in the event that the provider opened up ICUs to COVID-19 patients.
- Negotiated with several major health care providers and determined that this was the cost of increasing COVID-19 treatment.

Illinois.gov

Executive Order 2020-19 ^{April 1, 2020} EXECUTIVE ORDER 2020-19

EXECUTIVE ORDER IN RESPONSE TO COVID-19
(COVID-19 EXECUTIVE ORDER NO. 17)

WHEREAS, I, JB Pritzker, Governor of Illinois, declared all counties in the State of Illinois as a disaster area on March 9, 2020 (First Gubernatorial Disaster Proclamation) in response to the outbreak of Coronavirus Disease 2019 (COVID-19); and,

WHEREAS, I again declared all counties in the State of Illinois as a disaster area on April 1, 2020 (the Second Gubernatorial Disaster Proclamation, and, together with the First Gubernatorial Disaster Proclamation, the Gubernatorial Disaster Proclamations) in response to the exponential spread of COVID-19; and,

WHEREAS, in a short period of time, COVID-19 has rapidly spread throughout Illinois, necessitating updated and more stringent guidance from federal, state, and local public health officials; and,

WHEREAS, for the preservation of public health and safety throughout the entire State of Illinois, and to ensure that our healthcare delivery system is capable of serving those who are sick, I find it necessary to take additional measures consistent with public health guidance; and,

WHEREAS, ensuring the State of Illinois has adequate bed capacity, supplies, and providers to treat patients afflicted with COVID-19, as well as patients afflicted with other maladies, is of critical importance; and,

WHEREAS, eliminating obstacles or barriers to the provision of supplies and health care services is necessary to ensure the Illinois healthcare system has adequate capacity to provide care to all who need it; and,

WHEREAS, the Illinois Department of Financial and Professional Regulation and the Illinois Department of Public Health (DPH) have taken measures, and continue to take measures, to enable inactive and out-of-state health care workers to come back to work in the State of Illinois through proclamations, emergency rules and variances; and,

WHEREAS, DPH has taken measures, and continues to take measures, to enable hospitals to increase bed capacity and provide levels of care necessary to respond to the COVID-19 outbreak; and,

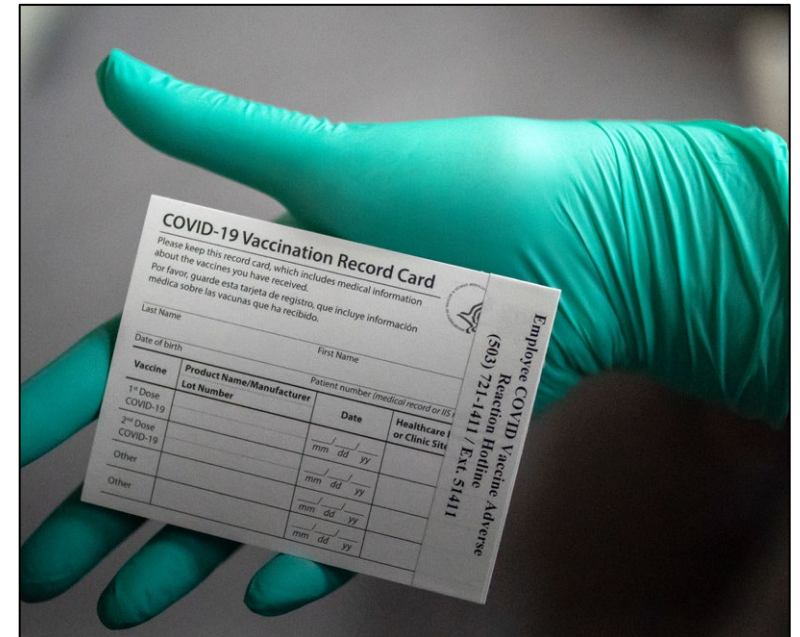
Poll Question #2

- Which area of post-pandemic litigation are you most concerned about?
 - A) Force Majeure
 - B) Data Privacy & Protection
 - C) COVID-19 Exposure civil actions
 - D) Other



Litigation Arising from the Pandemic

- **Employer & Employee Rights Regarding COVID-19 Vaccines**
 - Can employers mandate vaccinations?
 - Governmental guidance suggests an employer can mandate, if they provide accommodations or exemptions for:
 - Religious Beliefs (Title VII);
 - Disabilities (ADA);
 - If there are no state laws that preclude such a mandate.
 - Should employers mandate vaccinations?
 - Incentives – Encouraging, but not requiring vaccines.



CNA website back up two weeks after insurance giant hit with 'sophisticated ransomware attack'



- **Data Privacy & Information Protection**

- Reasons for Increased Cyber Attacks

- Federal Legislation

- State Legislation Regarding Data Breaches:

- Illinois Personal Information Protection Act
- Missouri - Mo. Rev. Stat. § 407.1500

RANSOMWARE

What It Is & What To Do About It

What is Ransomware?
Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Government Efforts to Combat Ransomware
While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact of ransomware on the networks of state, local, tribal, and territorial governments, municipalities, police and fire departments, hospitals, and other critical infrastructure. These types of attacks can delay a police or fire department's response to an emergency or prevent a hospital from accessing lifesaving equipment. To combat this threat, the NCJTF has convened an interagency group of subject matter experts to educate the public on ways to prevent ransomware attacks, to improve law enforcement coordination and response, and to enable and sequence whole-of-government actions that impose consequences against the criminals engaged in this malicious activity. The Cybersecurity and Infrastructure Security Agency (CISA) leads a number of efforts including [CISA Cyber Essentials](#) and [CISA Insights](#) to assist entities in protecting themselves from cyber incidents like ransomware. More about these efforts and the tools CISA offers can be found at <https://www.cisa.gov/ransomware>. The FBI's IC3.gov website has additional ransomware focused resources that can be found at <https://ic3.gov/Home/Ransomware>.

Common Infection Vectors
Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- **Email phishing campaigns:** The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.
- **Remote Desktop Protocol (RDP) vulnerabilities:** RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.
- **Software vulnerabilities:** Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

- Data Privacy & Information Protection
- American Bar Association Guidance
- Forensic Evaluation
- Potential Protections
 - Multi Factor Authentication
 - 24 Hour Monitoring
 - Encryption for PII

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction¹

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.² In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.³ Indeed,

enforcement officials regularly divide business entities hacked and those that will be.⁴

Committee explained a lawyer's ethical responsibility to use client confidential information using the Internet.⁵ This

Professional Conduct as amended by the ABA House of Delegates, regulations, rules of professional conduct and opinions regarding

Targeting Law Firms' Data (Aug. 3, 2017), <https://www.sio.com/newsroom/press-releases/2017/08/03/targeting-law-firms-data>

Request Network Breach for Insider Trading, Private Industry (Mar. 4, 2016), <https://www.sio.com/newsroom/press-releases/2016/03/04/request-network-breach-for-insider-trading-private-industry>

Firms, Including Cravath and Weil Gotshal, WAIJ, St. J. (Mar. 2, 2017), <https://www.sio.com/newsroom/press-releases/2017/03/02/firms-including-cravath-and-weil-gotshal-waij>

Cyber World Outsmarting Terrorists, Hackers and Spies, FBI (Oct. 17, 2017), <https://www.fbi.gov/newsroom/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

Formal Op. 477R (2017) ("Securing Communication of Protected Information")

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 498

March 10, 2021

Virtual Practice

The ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm.¹ When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.

I. Introduction

As lawyers increasingly use technology to practice virtually, they must remain cognizant of their ethical responsibilities. While the ABA Model Rules of Professional Conduct permit virtual practice, the Rules provide some minimum requirements and some of the Comments suggest best practices for virtual practice, particularly in the areas of competence, confidentiality, and supervision. These requirements and best practices are discussed in this opinion, although this opinion does not address every ethical issue arising in the virtual practice context.²

II. Virtual Practice: Commonly Implicated Model Rules

This opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional brick-and-mortar law firm.³ A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

² Interstate virtual practice, for instance, also implicates Model Rule of Professional Conduct 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law, which is not addressed by this opinion. See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 495 (2020), stating that "[l]awyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction."

³ See generally MODEL RULES OF PROFESSIONAL CONDUCT R. 1.0(c), defining a "firm" or "law firm" to be "a lawyer or lawyers in a partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization on the legal department of a corporation or other organization." Further guidance on what constitutes a firm is provided in Comments [2], [3], and [4] to Rule 1.0.

Practical Considerations Caused by COVID-19

- Encourage settlements due to inability to try a case.
- Alternative Dispute Resolution – mediation, arbitration.
- Lower costs for travel to courts, depositions, etc.
- Unable to move cases forward.
- Inability to obtain service of summons or service of writs (e.g. foreclosure/eviction).
- Increased use of technology in the courts (both positive and negative).
 - Juror irregularities during remote trials, internet connectivity, cat filters, etc.



Closing Remarks



SWANSON, MARTIN & BELL, LLP

Thank you!

John P. Arranz

312-321-9100

jarranz@smbtrials.com

www.smbtrials.com/jarranz

Robert W. Stephens

314-241-7100

rstephens@smbtrials.com

www.smbtrials.com/

Marcie J. Vantine

314-241-7100

mvantine@smbtrials.com

www.smbtrials.com/mvantine