Seyfarth

Commercial Litigation Outlook

2022 Edition

Commercial Litigation Outlook

Introduction

—By Shawn Wood and Rebecca Woods

Welcome to the second annual installment of Seyfarth Shaw's Commercial Litigation Outlook. Our nationally recognized team provides keen insights about what to expect in 2022. In short, it will be a busy year that will call upon clients and their counsel to be flexible, creative, and proactive on many fronts.

As the pandemic morphs into an endemic, we are seeing overall litigation activity increase as court backlogs have cleared and trials have resumed. The drivers of increased litigation are many, including vaccine availability, a more robust federal enforcement scheme, and impending court deadlines in cases that were either filed during the early stages of the pandemic or which had previously stalled due to restricted travel, inactivity, or court closures.

At the same time, we are living through a significant shift in how legal services are performed and delivered. Advances in technology and the pandemic's forced remote practice have accelerated innovation in practice tools, technological acumen, and flexible approaches. Piles of paper have been swapped for cloud-accessible and sharable work product. Flying lawyers all over the country to sit in conference rooms has been replaced, where strategically appropriate, by Zoom depositions and mediations. Lawyers and clients are seeing each other more, albeit via video. And for those companies and firms who committed to riding out the challenges of the past two years, collaboration has increased, even if we remain starved for more human interaction. Because many of these changes offer meaningful cost savings and streamlined processes and communications, they are—and should be—here to stay.

These innovations also bring certain risks. For example, there are significant questions around preservation and production of collaboration platform work (e.g., Microsoft Teams). A reliance on all things online, and remote workforces, has only amplified the risks around cyberattacks and privacy. Indeed, we anticipate seeing a significant increase in ransomware attacks, which are getting more extreme as they evolve toward exfiltration of data, as well as extortion. Employee training, and adequate cyber insurance, will be key tools to address these issues.

The cost and availability of insurance, meanwhile, becomes more difficult to navigate. Premiums are increasing across the board for all lines of insurance as insurers continue to labor in a low interest rate environment, pay out on significant climate-change-induced claims, and adjust their risk to the increase in expensive ransomware attacks.

We also anticipate a further proliferation of lawsuits due to government regulations adopted in response to evolutions in technology (e.g., biometric data), readily-shared personal information, the growth in health care fraud, and an increased sensitivity to privacy and consumer concerns. Companies operating in multiple states will want to stay abreast of continued legal changes in these spaces.

We also expect to see a more robust governmental focus on antitrust and consumer protection. On the other hand, over the last year, we have seen a slow-down in consumer and securities class actions, thanks in substantial part to federal relief efforts in connection with the pandemic, as well as a decrease in merger and acquisitions activity. With governmental relief ebbing and more M&A activity (including SPACs) increasing, we expect to see an uptick in these types of claims by mid-2022.

The new economy—and its effect on business models like franchising, staffing companies, and the sharing economy—continues to generate disputes around employee classification, allocation of liability, business model viability (and corresponding disclosures in purchases and sales), and social media presence and reputational management. Cryptocurrency, the epitome of the new economy, is also expected to generate challenges and opportunities for companies, both those directly involved in cryptocurrency and those who lean into taking it as payment.

Staying ahead of the curve in meeting these challenges remains our driving goal, as we work together to develop solutions and embrace new ways to navigate this rapidly changing landscape. We hope you will find this year's Commercial Litigation Outlook a useful resource in this regard, as well as an invitation for further discussion and collaboration.

We encourage you to contact any of the authors for assistance in connection with any of the areas of law or issues outlined here.

Cybersecurity and Privacy: Trends, Predictions, and Recommendations

— By Scott Carlson, Jason Priebe, and Emily Dorner

We can expect to see an increase in cybersecurity regulation at both the state and federal levels in 2022. In parallel, the debate of whether there will be a broad scale and all-encompassing data privacy law on the federal level will continue. Here are key trends, predictions, and recommendations.

CYBERSECURITY

2021 showed a tremendous increase in cybersecurity risk, with ransomware becoming a mainstream news topic. Organizations continue to recognize the threat, but all too often, do not do enough to address it.

Cybersecurity is often viewed as an IT risk, when in fact it is a business risk. Even when the risk is properly recognized, the efforts to improve security are often outstripped by the increased sophistication of threat actors. As is often heard in the world of terrorism, the threat actors only have to be lucky once, while the organization has to be lucky or prepared all the time. It is imperative that organizations take strong steps in 2022 to advance their cyber security maturity.

Ransomware has evolved to data exfiltration and extortion as well as ransomware as a service (RAAS)

Historically, ransomware focused on infiltrating organization endpoints and locking the organization out of their own data. While temporarily paralytic, organizations generally made it through those events by either paying the ransom or recovering their data from disaster recovery or backup media. Tactics have changed for many ransomware threat actors and will continue to evolve towards data exfiltration as a component of the ransomware attack. While the data is somewhat anecdotal as there is no central clearinghouse for reports of attacks, it was estimated that 50 percent of ransomware attacks in 2020 included data exfiltration. Many estimate that 80 percent of the attacks in 2021 included data exfiltration. As this appears to be the new tactic, we can expect 2022 to be worse. Once exfiltration is on the table, there is a substantial increase in the likelihood that (1) state data-breach notification statutes regarding the release of personal information will be triggered; (2) HIPAA notifications may be triggered for personal health information; and (3) domestic and foreign data privacy obligations will be triggered. This opens up the organization to increased risks of regulatory inquiry and class action lawsuits. Making matters worse, many threat actors have gone into the software business, providing RAAS, thereby allowing less-sophisticated threat actors to use their tool kits to execute attacks on their own using sophisticated software developed by others.

Email compromise events will continue to rise along with wire fraud

As we predicted for 2021, incidents involving threat actors gaining access to organizational email accounts will continue to rise in 2022. Unfortunately, organizations outside of the financial services industry have largely not improved dramatically. Password re-use, credential harvesting attacks, data leaks following a breach or extortion event, malware, phishing, smishing, etc., remain all too common. Once persistence is obtained in the environment, threat actors steal signature lines, email recipient metadata, prior dealing information, and payment information. This allows a threat actor to set up convincing-looking emails/invoices to perpetrate bank fraud. This comes in the form of requesting a fake invoice be paid or bank information changed. Unfortunately, this person-in-the-middle type attack often goes undetected by the employees involved.

The law remains largely unsettled as to who bears the risk of loss in such an attack. In 2022, organizations should focus on employee training to increase awareness, improve sophistication, and heighten their employees' "cyber-suspicion." Organizations will benefit from taking a closer look at their email system logging to ensure that requisite logs are available to conduct investigations following a business email compromise. Of all the areas of cyber risk, wire fraud is one where employee training and awareness can substantially reduce risk.

Cyber insurance will continue to be important with stricter underwriting requirements

Cyber insurance has become an increasingly common risk mitigation strategy for companies. However, cyber insurers are much more careful in their underwriting requirements, given the significant increase in claims and corresponding increase in ransomware payments in 2021. In 2022, the scope of underwriting investigation into the security program of the insureds will further intensify. Companies will be asked to provide detailed information regarding their risk profile, such as the amount of personal information they maintain as well as detailed information about their security program. They may ask for proof of cybersecurity risk assessments, penetration tests, NIST (or other framework) compliance, etc. Organizations who rely solely on cyber insurance coverage as their threat mitigation strategy may see their coverages shrink, sublimits increase, and rates increase.

Training remains a high priority

Technologic solutions alone cannot prevent cybersecurity threats, and employees will routinely be fooled by clever attacks. However, employee training will remain critical. Many of the most successful hacks to date have started with social engineering. Whether phishing, smishing, linkclicking, or myriad other methods, employees who are well trained will help their organizations avoid costly cybersecurity events. While technology advancements in early detection and containment will continue in 2022, the human elements in an organization cannot be abandoned. Reputable cybersecurity training providers will likely see an uptick in business as organizations move to defend their perimeters.

Governmental regulation will increase

At this point, all fifty states have data breach notification statutes. States are increasingly developing data privacy statutes. Following the Colonial Pipeline incident of 2021, bipartisan efforts are underway in Congress to pass a law requiring some sort of data breach notification to federal authorities. While it is difficult to predict what form those regulations will take, it seems clear that we can expect to see an increase in regulation at both the state and federal levels in 2022.

DATA PRIVACY

Each year includes a debate of whether there will be a broad scale and all-encompassing data privacy law on the federal level. And each year there are few updates to report, beyond existing federal regimes, to protect categories of information in various regulated industries, such as financial and consumer credit (e.g., GLB and FCRA); healthcare and related services (e.g., HIPAA); telecommunications; etc. As a midterm election year, 2022 has even less of a chance to see the introduction of any federal consumer privacy law. Potentially because of the years of inactivity at the federal level, many privacy advocacy organizations have turned to state legislatures and sought the passage of new consumer-oriented privacy laws, along with amendments to existing breach notification laws in order to strengthen consumer rights.

2021 saw continued and expected growth in the realm of state privacy laws. Most notably with Colorado and Virginia passing their first consumer-oriented privacy laws and California voting in November to expand upon consumer rights provided by the California Consumer Privacy Act (CCPA) with passage of the California Privacy Rights Act (CPRA). While these three new laws will not go into effect until 2023, there are a number of actions companies with a physical presence or covered activities in those jurisdictions should be taking to prepare for them.

New and amended distinctions for Sensitive Personal Information

As a further echo of the categorization and treatment for personal information based on the risk and sensitivity, we have seen in the past year a trend toward inclusion of "Sensitive Personal Information" as a separate and distinct category of personal information, carrying with it its own special protections. The CPRA, Virginia Consumer Data Protection Act (CDPA), and Colorado Privacy Act (CPA) each call out Sensitive Personal Information with similar but slightly varying definitions. *See* Cal. Civ. Code. Sec. 1798.185 (2020); Va. Code. Ann. Sec. §59.1-576 (2021); Colo. Rev. Stat. § 6-1-1309 (2021). The laws tend to place additional storage, notification, disclosure, retention, and purpose restraints on Sensitive Personal Information, as a means of allocating risk and security prioritization.

Privacy risk and impact assessments

Each of the three new state privacy laws requires an independent and documented risk assessment procedure related to certain types of processing of personal information. For example, under CPRA, cybersecurity audits and risk assessments will be required for companies whose processing presents "a significant risk to consumer privacy or security." Cal. Civ. Code. Sec. 1798.185 (a)(15) (2020). Likewise, the CPA will require a data protection assessment when a company engages in the processing of personal data for targeted advertising, the sale of personal data, the processing of personal data for purposes of profiling, the processing of sensitive data, or processing activities involving personal data that present a heightened risk of harm to consumers. Colo. Rev. Stat. § 6-1-1309 (2021). Virginia's CDPA will require the same before engaging in processing that presents a heightened risk of harm to a consumer. Under CDPA, "heightened risk to a consumer" includes processing personal data for purposes of targeted advertising or profiling, selling personal data, and processing sensitive data. Va. Code. Ann. Sec. §59.1-576 (2021).

Additional protection for personal information from minors

The three laws continue the trend we have observed over the past few years restricting the processing of personal data of children. These include, for example, heightened consent requirements, usually by the parent, and the classification of children's data as "sensitive." *See* Va. Code. Ann. Sec. §59.1-574(A); Colo. Rev. Stat. §6-1-1308(7); Cal. Civ. Code Sec. 1798.120. We expect to see additional restrictions on the collection and use of information from minors as individual states continue to propose their own privacy legislation, along with certain heightened consumer rights and requirements of notice, particular legal bases for processing, and obligations regarding the processing, transfer, and protection of personal information.

Additional breach response and notification requirements

There were changes to state law related to breach notification in 2021 that will have ramifications in 2022. Both Connecticut and Texas updated their breach notification laws. Specifically, Connecticut brought its breach notification law "up to date" with trends that other states had set, such as broadening its application, expanding the definition of personal information under the law, shortening the notice period to 60 days, and requiring credit monitoring when a social security number is breached, among other things. Conn. Gen. Stat. Sec. 36a-701b.

Texas, on the other hand, made more subtle changes, including updating the information required to be conveyed to the Attorney General when a breach occurs and updating requirements of the Attorney General to post information regarding breaches within 30 days. Of note, this Texas update follows a 2019 amendment that decreased the amount of time companies have to notify individuals (as well as the Attorney General) whose sensitive personal information was, or is reasonably believed to have been, breached. The amendment also established the Texas Privacy Protection Advisory Council to study data privacy laws in Texas. Tex. Bus. & Com. Code Sec. 521.053 (2021).

We expect to see a trend in the coming years of more states looking to update their breach notification laws in a similar manner to Connecticut. For example, we expect to see expanded definitions of personal information, as well as separate and distinct definitions of sensitive personal information, likely with differing requirements for reporting for personal and sensitive personal information. We also expect states to be more stringent about the timeframes in which a company must report a breach, a 45-60 day timeframe, rather than the vaguely defined "without unreasonable delay" that we commonly see. Finally, we also expect states to lower the threshold for attorney general or other supervisory authority reporting. While we don't expect to see timeframes as narrow as that imposed by the General Data Protection Regulation (GDPR) in Europe (72 hours), we do expect states to lower the threshold of individuals impacted to trigger a reporting obligation.

Recommended measures for 2022

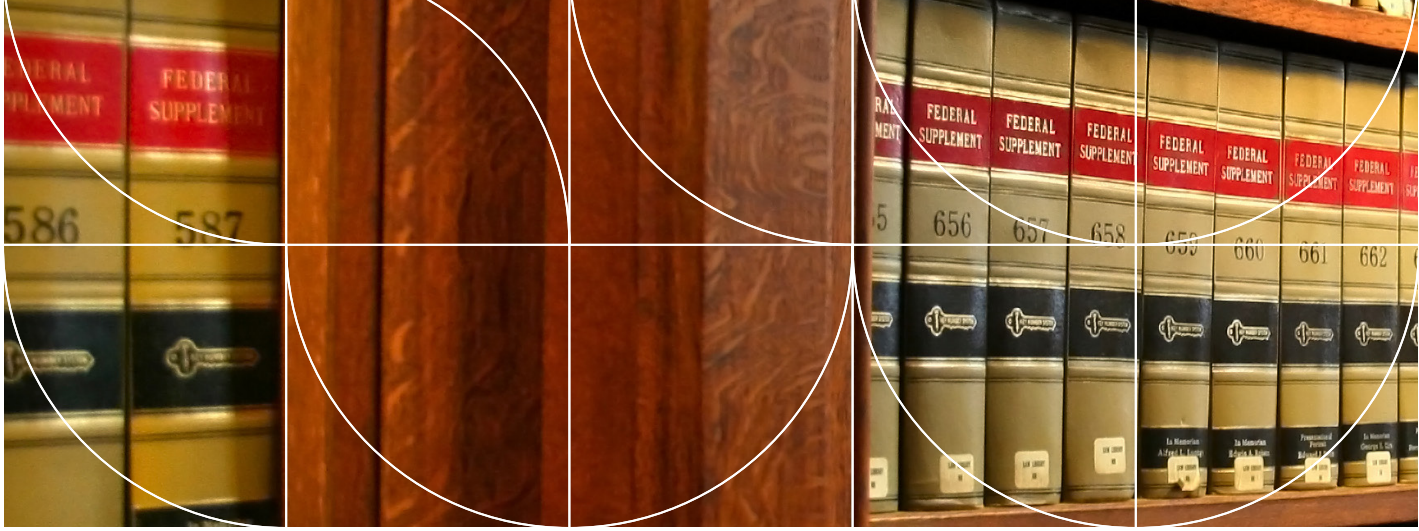
In order to prepare for these upcoming changes in these specific states, and likely more to come, Seyfarth recommends the following:

1. Assess whether the CDPA, CPRA, or CPA will apply to your organization;

2. If upcoming changes to state privacy laws do apply to your company, review those requirements and begin to prepare updated internal processes and procedures to ensure compliance starting in 2023; and

3. Conduct frequent IT and data security audits to aid in the prevention of data incidents, and update internal policies and procedures regarding data security and incident response to ensure the same are aligned with your company's sector-specific obligations.

In sum, we see 2022 as a proactive year in terms of privacy initiatives. Organizations should take advantage of the time afforded this year to prepare for the implementation of new laws in both the consumer privacy and data breach sectors, rather than reacting when they receive their first consumer access request for personal information or experience a breach and risk missing a supervisory reporting deadline.



Key Trends in Commercial Litigation

Antitrust

— By William Berkowitz, Brandon Bigelow, and Caleb Schillinger

Companies in all sectors should expect that regulatory review of proposed mergers and acquisitions will take longer and involve heightened scrutiny.

More aggressive enforcement of the federal antitrust laws is expected in 2022, with the US Department of Justice (DOJ) continuing to prioritize investigations of wage-fixing and no-poach agreements among employers in labor markets and the Federal Trade Commission (FTC) now focusing on unlawful repair restrictions in addition to greater scrutiny of proposed mergers.

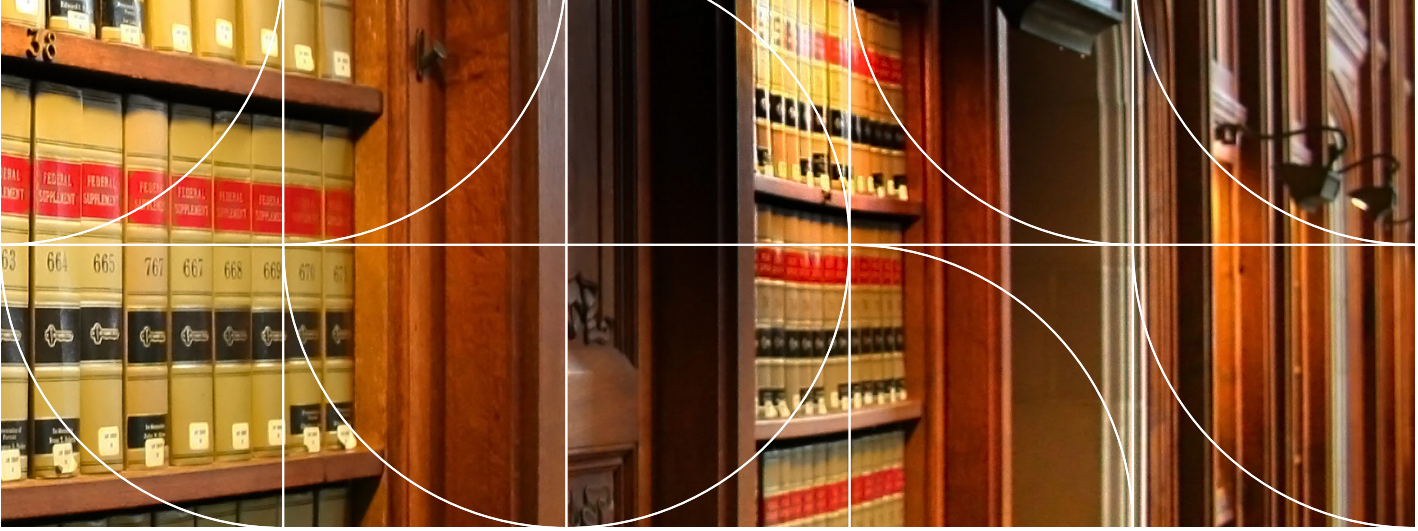
DOJ's criminal prosecutions of alleged collusion by employers

The DOJ had warned in 2016 in its Antitrust Guidance for Human Resource Professionals that the antitrust laws apply to competition among firms to hire employees and that the DOJ would bring criminal charges "against naked wage-fixing or no-poaching agreements." Companies cannot afford to take the DOJ's warning lightly—in December 2020, the DOJ filed criminal charges against the former owner of a therapist staffing company based on an alleged scheme to fix the wages paid to physical therapists and therapist assistants in the Dallas-Fort Worth area. In November 2021, the court in that case denied a defense motion to dismiss, finding that "[j]ust because this is the first time the Government has prosecuted for this type of offense does not mean that the conduct at issue has not been illegal until now. Rather … price-fixing agreements—even among buyers in the labor market—have been per se illegal for years."

The DOJ has since filed two additional criminal complaints against health care companies for allegedly entering into no-poach agreements with competitors not to solicit or hire each other's employees, and wage-fixing and no-poach agreements will continue to be an antitrust enforcement priority for regulators in 2022. These enforcement actions are more likely than ever to take the form of criminal prosecutions. One important step all companies can take to significantly reduce antitrust risk is to maintain a robust antitrust compliance policy, supported by regular programs and trainings. In 2019, the DOJ announced a new policy that directs prosecutors to consider the adequacy and effectiveness of a corporation's compliance program at the charging stage in criminal antitrust cases, meaning that businesses that take antitrust compliance seriously may be able to avoid the worst consequences even if rogue employees violate the antitrust laws.

FTC's increased scrutiny of repair restrictions

On July 9, 2021, President Biden issued an "Executive Order on Promoting Competition in the American Economy," which directed federal agencies to ramp up their enforcement of the antitrust laws (and other industry-specific competition statutes) in order to combat the perceived "excessive concentration of industry, the abuses of market power, and the harmful effects of monopoly and monopsony" in a variety of markets, including "repair markets." Soon thereafter, the FTC released a policy statement on "Repair Restrictions Imposed by Manufacturers and Sellers," in which the agency said it "will scrutinize repair restrictions for violations of the antitrust laws" and "prioritize investigations into unlawful repair restrictions." One such restriction highlighted in the policy statement is a "tying arrangement" that "condition[s] a consumer product's warranty on the use of a third-party service provider or on the use of a particular product," in violation of the Magnuson-Moss Warranty Act, the Sherman Act, and Section 5 of the FTC Act.

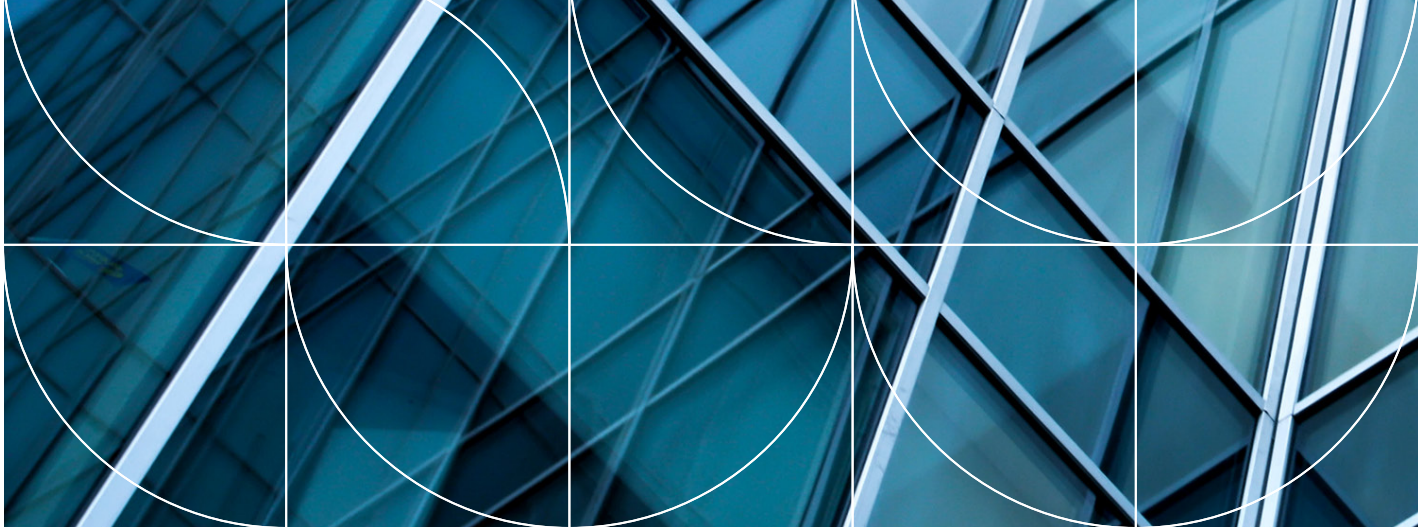


The FTC's policy statement builds off of the agency's prior "Nixing the Fix" workshop and report to Congress on repair restrictions. Through that work, the FTC claims to have uncovered evidence that manufacturers and sellers may, without reasonable justification, be restricting competition for repair services in numerous ways, including: imposing physical restrictions; limiting the availability of parts, manuals, diagnostic software, and tools to manufacturers' authorized repair networks; using designs that make independent repairs less safe; limiting the availability of telematics information; asserting patent rights and enforcement of trademarks in an unlawful, overbroad manner; disparaging non-OEM parts and independent repair; using unjustified software locks, digital rights management, and technical protection measurers; and imposing restrictive end user license agreements. Given the FTC's stated intent to increase its scrutiny of repair restrictions, manufacturers would do well to review their written warranties and internal warranty policies and procedures to ensure they comply with all applicable laws.

> One important step all companies can take to significantly reduce antitrust risk is to maintain a robust antitrust compliance policy, supported by regular programs and trainings.

FTC's heightened review of proposed mergers

This past year also saw the FTC implement significant changes to its review of proposed mergers and acquisitions that could impact transactions occurring in 2022. In February 2021, the agency suspended (indefinitely) the granting of early termination of the 30-day waiting period under the Hart-Scott-Rodino Antitrust Improvements Act. In August 2021, citing a recent "tidal wave" in merger filings, the FTC said that in instances where it could not complete its investigation of a proposed transaction within the 30-day period, it had begun to send a standard form letter alerting the parties that the agency's investigation remained open and "companies that choose to proceed with transactions that have not been fully investigated are doing so at their own risk." In October 2021, the FTC announced that it was "returning" to its "prior practice of routinely requiring merging parties subject to a Commission order to obtain prior approval from the FTC before closing any future transaction affecting each relevant market for which a violation was alleged" by "rescinding" a 1995 FTC policy statement that had ended that practice. The upshot of these changes is that companies in all sectors should expect that regulatory review of proposed mergers and acquisitions will take longer and involve heightened scrutiny.



Key Trends in Commercial Litigation

Bankruptcy

— By Bill Hanlon

Bankruptcy filings hit record lows in 2021; for 2022, we anticipate an increase in filings caused by the end of stimulus funding, reopening of courts, a renewed willingness to enforce creditor remedies, among other trends.

Bankruptcy filings hit record lows in 2021 thanks to stimulus funding; court closures; student loan, eviction, and foreclosure moratoria; and a willingness among debtors and creditors to work out their issues. With courts closed and reluctant or stayed from enforcing creditor rights, fewer entities needed to invoke the automatic stay, a chief benefit of filing bankruptcy.

For 2022, we anticipate an increase in filings caused by the end of stimulus funding (particularly PPP loans), reopening of courts, a renewed willingness to enforce creditor remedies, the expiration of moratoria, supply chain pressures, rising inflation, and increased interest rates. These external pressures will cause an increase in bankruptcy filings. Bankruptcy filings by debtors in response to fraud and unique causes will continue at their usual rate.

Real Estate

Delinquency rates for CMBS loans dropped from a COVID-19 high of 10.32% in June 2020 to 5.25% in September 2021. (For comparison sake, the all-time high delinquency rate was 10.34% in July 2012.) The most stressed sectors are retail and lodging. Most industry experts expect a rise in office delinquencies, continued turbulence in the business hospitality and lodging sectors, and declining delinquencies in the retail sector, which has seen considerable shake-out in the past several years.

It's no secret that low interest rates and large amounts of liquidity in the markets have pushed real property prices very high. Many of our business colleagues report that buyers are resorting to "creative" financing solutions, including multiple layers of debt, participation loans, use of preferred equity, and mezzanine financing to purchase properties in an over-heated marketplace. To anyone who has lived through a real estate cycle, "creative" financing is a harbinger of a down cycle. Once a borrower and lender move past "extend and pretend" forbearance, litigable issues arise upon enforcement. We expect litigation over enforcement of mezzanine debt a/k/a "equity clogging," election of remedies, compliance with the patchwork of state and local restrictions on foreclosure, as well as disputes between creditors over priority and control of collateral. Additionally, borrowers carefully structured as bankruptcy remote at origination, often arrive in bankruptcy court in breach of their separateness covenants, which may give rise to disputes over borrower's eligibility for bankruptcy relief and requests substantive consolidation as a stepping stone to "cramming down" secured lender's claims.

Health Care

COVID-19 caused a focus on operations, not long-term business; for example, businesses focused on managing cash flow issues due to a decrease in elective procedures

and an increase in the need to purchase protective gear and hospital staff. These issues were mitigated by the CARES Act and, more recently, the resumption of elective procedures. The Delta (and now Omicron) variant has emerged and reversed some of this progress, but if this can be brought under control, we can look forward to expansion of mergers and acquisitions and continuing divesting of non-performing or underperforming assets, particularly in the skilled nursing and home health areas. A lot of stimulus went toward avoiding hospital and nursing home closings during the pandemic. The stimulus is not forever, and the lack of elective procedures, mediocre reimbursement rates, and lack of staffing may catch up with the industry in 2022 and lead to insolvencies, transfers, or liquidation of health care facilities in bankruptcy cases, or more commonly, receiverships.

Long-term issues will continue to affect the health care sector. Continuing care is over-bedded in most states and dependent upon private payors rather than government reimbursement. Staffing will be a continuing crisis—there are simply not enough trained medical staff for current needs, and those working throughout the pandemic are suffering from fatigue. The surge in the Delta and Omicron variants is taking up resources otherwise utilized in elective procedures and routine health care, limiting some of the more profitable practices. Rural hospitals and skilled nursing homes are most likely to be undercapitalized, short staffed, and subject to declining reimbursement rates. These are the entities most likely to fail in the years ahead as the stimulus dries up. Legal issues abound: a sale "free and clear" of Medicare and Medicaid recoupment and set-off rights is far from a forgone conclusion, which can saddle the acquirer of medical assets with debt from the distressed entity; courts often conclude that a provider's participation in Medicare is a single, integrated transaction which permits the government to recover advances notwithstanding bankruptcy. Additional litigable issues triggered by closings and transfers include: jurisdiction of receivers, oversight of patient care, transfer of patients from failed facilities, protection of personally identifiable information, priority of loan advances made to continue operations, indemnity between old and new operators, control and collection of receivables, and exercise of setoff rights.

The end to forbearance?

In 2022, we expect a decline in forbearance and an increase in enforcement, which will cause a gradual increase in litigation and then bankruptcy cases in late 2022 and 2023. Unlike 1987's Black Monday, 1990's oil and housing bubble, and 2001's dot-com bust, the current pandemic's financial disruption arises from a morally neutral cause, and with liberal stimulus and moratoria, has resulted in an extended period of forbearance and forgiveness. The stimulus is largely gone. The Federal Reserve is expected to raise interest rates. Supply chain and labor shortages are inhibiting financial performance. Lenders often focus on problem loans in the second and third quarters in anticipation of annual reporting on goals and performance in the fourth quarter. Once a loan transfers to "special servicing," enforcement efforts typically escalate, and when they fail, the result is often litigation. Creditor remedies take time to enforce. Debtors typically exhaust all options before invoking the automatic stay. Historically, Bankruptcy Court is the court of last resort for most debtors, and we expect it will be so here.

Key Trends in Commercial Litigation

Consumer Class Action Defense

— By Kristine Argentine, Emily Dorner, and Paul Yovanic

As courts across the country are grappling with how to operate amidst the health risks and backlogs created over the past two years, consumer class actions continue to be filed at an alarming rate.

Although the pandemic still lingers and the courts across the country are still grappling with how to operate amidst the health risks and backlogs created over the past two years, consumer class actions continue to be filed at an alarming rate. The trend of consumer class actions will continue in 2022, and this past year brought some clarity regarding where the Plaintiffs' bar will likely focus and what we can expect in the upcoming year.

The major decisions in 2021 signal a shift in the way courts will view class actions from a procedural perspective. Perhaps most significantly, the Supreme Court in *TransUnion* clarified Article III standing. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 210 L. Ed. 2d 568 (2021). Specifically, the court held that Article III standing is limited to only those class members that demonstrate injury in fact, meaning that the injury should not be based solely on a statutory right to sue. The Supreme Court further clarified that every class member, not just the named plaintiffs, must show a concrete injury. This decision, which disallows bare allegations of statutory violations without actual harm, means that the battlefield for consumer class actions will likely shift in 2022 to state courts in cases where the alleged harm is based only in statute or the risk of future harm is speculative.

For those class actions that remain in federal court, the circuits have started to move away from the heightened ascertainability standard which required that the plaintiff show that the class could be easily identified from specific documents or information. Rather, courts are only requiring that the class be clearly defined for purposes of class certification. The changing views with respect to ascertainability at the class certification stage will make it easier for the Plaintiffs' bar to achieve certification and increase the risk of liability and potential defense strategies at the outset of these cases.

New twist on data collection claims

One trend that emerged in the consumer class action space in 2021 was the filing of wiretap claims against large commercial website operators. These class actions alleged that the use of "session reply" technology, which captures consumer keystrokes and mouse clicks, violate state wiretap statutes by recording the consumer's interactions with the website. These cases started in California, and quickly, dozens of class actions were filed in Florida. This, however, may only be the tip of the iceberg, as at least 15 states require consent from all parties when a communication is recorded or intercepted. Further, penalties in two-party consent states are steep, ranging from $1,000 to $5,000 per violation.

The inevitable challenge with these types of claims is that the wiretap acts are decades old and the language does not address modern technology. As these cases make their way through the courts, a body of defense- friendly case law is developing such that early dismissal in these cases may be possible. Courts appear ready to find that session replay software does not intercept the "contents" of a user's communication and that session replay software is not a "device" within the meaning of the statute. However, not all courts are in accord and we expect plaintiffs will continue to push wiretap suits in non-hostile jurisdictions.

One way companies can protect themselves from these type of claims in 2022 is to update terms of use and privacy policies to include specific consents to the use of session replay and similar technology and include additional disclosures related to information that may be collected through their website.

Cyber-related class actions

Over the past year, there has been a dramatic increase in cyber-related class actions. Much of this is driven by FTC guidelines that focus on protecting personal information, and plaintiffs' counsel are using those guidelines as the "standard of care" that should be met in protecting consumer information. Because there may be traction in this space, we expect to see the hotly-litigated procedural challenges to continue, especially with respect to class certification, standing, and the discoverability of forensic reports.

In 2021, for the first time, a damages class action for data breach was certified under Federal Rule 23(b)(3). Here, the court took an unconventional approach, evaluating plaintiff's ability to pursue their claims outside of class action, and only granted certification on negligence claims. Although this was the first decision of its kind, we expect plaintiffs to continue to press in this space.

We expect to see continued energy from the plaintiffs' bar because there is a circuit split on the harm required in order to trigger Article III standing, and a 2021 decision from the US Supreme Court offered little in the way of clarity. Here, the Supreme Court looked to the issue of standing and "injury in fact," which was a novel issue for the Court in the context of a data breach suit. Here, the Supreme Court found that certain consumers whose information was divulged to third party businesses had indeed suffered a concrete injury in fact; the Court, however, did not take up an analysis of whether future risks of harm give rise to standing—an argument frequently pursued by plaintiffs in breach cases. The Supreme Court did note, however, that aside from physical or financial harm, reputational harm, the disclosure of private information, or intrusion upon seclusion may rise to the level of concrete harm. *Id*. This provides some interesting context into what we might see in 2022 and beyond and begs the question of whether a "risk of harm analysis" might be necessary in the context of a breach, where private information is indeed accessed and disclosed (i.e., disseminated) to an unauthorized third party. We expect contention to continue on this front, with plaintiffs continuing to bring suit based on a future risk that their personal information may be misused, or instead utilizing the Supreme Court's definition of a concrete harm, specifically their mention of the disclosure of private information, to argue that a disclosure will give rise to a concrete harm, and therefore conveys Article III standing.

Finally, we expect to see parties continue to challenge the sufficiency of claims of attorney-client privilege over forensic reports that are prepared in response to data breaches. For example, in August of 2021, a magistrate judge in the Middle District of Pennsylvania ordered a party to produce a cybersecurity report prepared by a vendor engaged by the party's counsel because the court found that the report was not protected under either the work-product doctrine or the attorney-client privilege. While traditional forensic reports contain important information requiring protection, states continue to enact privacy laws that are geared toward the principle of transparency and undermine claims of privilege. As a result, when forensic reporting is carried out as part of incident response, rather than in the anticipation of litigation, (regardless of whether a law firm was also engaged and providing direction and legal advice), we expect to see a decline in privilege protection over these reports. Fortunately, recent case law demonstrates certain steps that companies experiencing data incidents can take to ensure that privilege is protected for forensic reports prepared when litigation is expected. Most importantly, we recommend that a clear line be drawn between a forensic investigation for incident response, and one performed in anticipation of litigation. In order to accomplish this, organizations should consider:

- Engaging separate vendors and/or law firms for forensic analysis in the context of potential litigation
- The budget from which law firms and forensic vendors are paid for forensic analysis and work
- Whether it is possible for the engaged law firm to hire the forensic vendor
- Internal stakeholders with whom it is necessary to share potentially-privileged forensic reports
- Whether a written forensic report is necessary, or whether a verbal report is more appropriate and can accomplish the same objective

While these steps will not guarantee that privilege may be maintained over such reports, they'll strengthen any arguments should plaintiff's counsel challenge any assertions of privilege.

Telephone Consumer Protection Act litigation continues

We expect federal Telephone Consumer Protection Act (TCPA) claims to reduce, thanks to a defense-friendly Supreme Court ruling, but state TCPA-like litigation to grow.

TCPA class actions have dominated the consumer class action space because of the large number of technical requirements and the high statutory damages. The Supreme Court's ruling in 2021 redefining automatic telephone dialing systems under the TCPA was a huge win for defendants. In its ruling, the Court found "that a necessary feature of an autodialer is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called." This definition of an autodialer was a significant departure from the previously followed view that an autodialer was any device that could automatically dial a number, which effectively included every smartphone. Since this ruling, courts across the country have consistently been using this

Key Trends in Commercial Litigation

Consumer Class Action Defense (cont.)

decision to dispose of TCPA cases at the summary judgment, or even the motion to dismiss, stage.

We expect federal TCPA claims to persist because some courts have not been as quick to accept the Supreme Court's decision, especially at the pleading stage, because courts are still finding that whether a device constitutes an autodialer requires technical knowledge that a plaintiff is not required to have at the pleading stage. These courts are allowing bare bones pleading about the defendant's "use of an autodialer" to survive. Additionally, we expect to see increased litigation at the state level because some states have started to amend their telecommunications laws and mini-TCPA statutes to allow private rights of action under those statutes. Many of these amendments do not adhere to the strict definition of an autodialer deemed to be the requirement in the TCPA by the Supreme Court. Specifically, in July 2021, Florida amended its state telecommunications laws to add a private right of action. The Florida statute prohibits telephonic sales calls and texts without the prior express consent of the called party and does not limit its application to automatic telephone dialing systems (autodialers or ATDS). Dozens of class actions have already been filed pursuant to the Florida statute. Similarly, in July 2021, New York amended its telemarking laws to include "electronic messaging text" in its definition of telemarketing. We expect that more states will amend their telemarketing laws to further restrict calls and texts to consumers and possibly allow private rights of action for violations. Other states that have broader statutes include Washington, Virginia, and Texas. Importantly, the TCPA does not preempt state law that imposes more restrictive provisions than the TCPA. Thus, states may become the new battle ground for the plaintiffs' bar on text and robocall claims, especially as states continue to alter their statutes to be more restrictive than the TCPA.

Additionally, in 2022, the Plaintiffs' bar will likely shift tactics in its pursuit of TCPA violations, focusing more on pre-recorded calls and violations of the Do Not Call registry, neither of which require the use of an autodialer to prove a violation. The TCPA also contains a host of other technical requirements around abandon calls, internal Do Not Call lists, and regulated calling hours.

One other update that will affect the landscape of TCPA claims in 2022 is the use of a defense when a business calls a number for which it believes it has consent, but the number was reassigned. Reassignment of numbers is, to date, not a defense, and calls to that number are treated as a strict liability offense. On November 1, 2021, however, a reassigned number database went live, and it tracks all cell phone reassignments in the United States, and it will provide a user with information as to whether a particular number has been reassigned. Thus, a caller can scrub its lists of phone numbers against the database to know whether any of the numbers it intends to call are no longer assigned to the consumer they believe they are calling or texting. Importantly, the FCC has issued a safe harbor that would shield a caller from liability if the caller used the reassigned number database to check the numbers it was calling and the information provided was inaccurate. In 2022, we expect to see various defenses raised related to the use of the reassigned number database and the triggering of the safe harbor provided by the FCC.

Biometric privacy legislative update

This year has remained busy for biometric protection as Portland, Oregon, and New York City joined the growing trend and enacted ordinances closely following the highly-litigated Illinois Biometric Information Privacy Act (BIPA). We can and should expect the Plaintiffs' bar to capitalize on these biometric laws, particularly due to the attorneys' fee provisions.

Portland's ordinance (Ch. 34.10) went into effect on January 1, 2021, and bans private entities from using any facial recognition technology in any "places of public accommodation," with limited exceptions, such as when it is necessary to comply

with federal, state, or local laws. Private entities are subject to the ordinance if they constitute a "place[] of public accommodation," which essentially encompasses a ban on all types of businesses—including banks, hotels, convenience stores, just to name a few—that are now completely barred from using facial recognition for any purpose. The ordinance creates a private right of action for actual damages sustained as a result of the violation or $1,000 per day for each day of violation, whichever is greater, as well as attorneys' fees to a prevailing party. The broad definition of "places of public accommodation" and the draconian damages provision are likely to lead to an explosion of litigation of the ordinance.

Effective July 1, 2021, New York City's ordinance (§22-1201 et seq.) placed new obligations on businesses to notify customers and potential customers if they collect biometric information "by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances." The ordinance provides for a private right action and permits the individual to recover $500 for each negligent violation and up to $5,000 for each intentional or reckless violation of the ordinance, in addition to reasonable attorneys' fees. While the New York City ordinance differs from Portland's, in that it does not place an outright ban on the collection of biometric information, businesses that are considered a commercial establishment will likely be drawn into litigation in large part due to the damages provision. Like BIPA, there are likely going to be disputes as to what constitutes a negligent violation compared to a reckless violation, whether a violation occurs each time a customer enters a commercial establishment that collects biometric information, and whether the establishment placed a notice sign in a clear and conspicuous manner.

Those businesses familiar with BIPA have seen these cases survive the pleading stage in Illinois courts, often reaching class certification. Just as BIPA resulted in myriad class action lawsuits and harsh and unwavering penalties, we expect a similar waive of litigation in Portland and New York City. Thus, it is more important now than ever for businesses to understand and comply with biometric privacy laws in each state where they are operating. This should extend to the adoption of practices and policies relating to the collection, storage, and retention of biometric information, as well as avoiding or disabling technologies that unnecessarily collect such data to ensure continuing compliance with governing state statutes or (now) local ordinances.

Key Trends in Commercial Litigation

Consumer Financial Services Litigation

— By David Bizar and Tonya Esposito

What to expect this year in government enforcement litigation, civil litigation and class actions, and FinTech.

Consumer financial services providers are subject to regulations and claims specific to their industries and products. Consumer finance products include secured loans, like mortgages and auto loans, and unsecured loans, like student loans and credit cards. Regulators and enforcement authorities of consumer financial providers include the Consumer Financial Protection Bureau (CFPB), United States Department of Justice (DOJ), Federal Trade Commission (FTC), Office of the Comptroller of the Currency (OCC), State departments of banking and finance, and State attorney's general.

Government enforcement litigation

Government enforcement litigation experienced an uptick in 2021 and is expected to increase more substantially in 2022. The CFPB is expected to up its enforcement activities in 2022 with an emphasis on repeat offenders, particularly those that violate agency or federal court orders, or on matters that concern technology or data. In late 2021, the DOJ announced a new, joint "Combatting Redlining Initiative" by the Attorney General of the United States, which combines DOJ's resources and enforcement efforts with that of the CFPB and OCC, to "represent[] the department's most aggressive and coordinated effort to address redlining, which is prohibited by the Fair Housing Act and Equal Credit Opportunity Act." The Initiative's focus is on redlining by algorithm, in which lenders are alleged to rely on computerized data to avoid providing loans to persons living in communities of color because of the race or national origin. The OCC is expected to make the Initiative a priority, and to focus on new bank regulatory efforts recognizing climate change, and regulation of cryptocurrency and synthetic banking providers, as its Acting Comptroller has previously called for. The FTC has also signaled a more aggressive approach to consumer protection enforcement, with its chair reportedly stating a concern regarding the "existential stakes of underreaching or 'neutering the tools' available to the agency."

On April 22, 2021, the United States Supreme Court held in *AMG Capital Management, LLC v. FTC* that the FTC could not use its Section 13(b) authority to seek monetary penalty violations for violations of the FTC Act. But the FTC has sought another route to recover civil penalties within the last year, by reviving the agency's long-dormant Penalty Offense Authority under Section 5(m)(1)(B) of the FTC Act (45 U.S.C. § 45(m)(1)(B)), which allows the Commission to pursue civil penalties in federal court for knowing violations of the FTC Act. Various media reports state that in 2021, the FTC sent various Notice of Penalty Offenses to 2,000 businesses and 70 for-profit higher educational organizations. Such notices do not allege that the recipients engaged in wrongdoing, but state that the recipient may incur significant civil penalties of up to $43,792 per violation if they do engage in wrongdoing. The FTC issues these notices in order to take the position in a future investigation or enforcement action that the recipient possessed actual knowledge of wrongfulness of the conduct at issue, following its receipt of the notice. These notices are thought to communicate to industry participants that the FTC intends to engage in additional enforcement activity. While the FTC's notices in 2021 did not target consumer finance companies per se, the FTC is expected to focus on the technology industry and business unfair trade practices, particularly in relation to larger businesses.

State departments of banking and state attorney's general are also likely to remain actively engaged, as they have been historically, in investigating and enforcing claims of consumer protection law violations.

Civil litigation and class actions

The primary driver of consumer finance civil disputes is distressed consumer debt. A consumer fails to pay back a personal loan. The lender demands payment or seeks to recover its collateral for the default. The consumer responds by filing a lawsuit or counterclaim or makes a complaint to a government agency. Typically, the consumer asserts an illegality regarding whether the loan should have been made or the loan product's terms or disclosures. In other instances, the consumer challenges the lender's servicing or collection practices. Frequently, the consumer brings the lawsuit as a class action on behalf of all similarly situated persons, or asserts the claims individually but the claims have systemic exposure for the lender. This means that if the lender is held liable for the claims in a final judgment, other borrowers can then utilize the judgment to sue for themselves, or through filing a class action, for also being victims of the adjudged illegality.

We expect consumer financial services civil litigation to begin to pick up in 2022 as government assistance programs implemented during the COVID-19 pandemic conclude. Federal relief efforts through the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), signed into law on March 27, 2020, and follow-on legislation, have been the largest economic stimulus in US history, injecting at least $5.2 trillion into the US economy through 2021. The federal government has provided substantial cash payments and other relief to help consumers to pay their bills, including their loan payments. The government also mandated that a mortgage payment forbearance option be provided to any borrower of a federally-backed mortgage loan (at least 75% of all consumer residential mortgage loans) who self-certified to their mortgage servicer by June 20, 2021, that they either directly or indirectly suffered a financial hardship due to the COVID-19 emergency. Forbearances can be extended for up to 18 months, with many financial institutions expanding such relief to their entire portfolio of mortgage loans. The Mortgage Bankers Association issued its final Forbearance and Call Volume Survey on November 8, 2021, reporting that there were one million homeowners on forbearance plans, down from over six million in mid-2020. This downward trend is expected to continue in 2022, as borrowers whose loans are coming out of forbearance have their loans modified by their lenders to lower their payment obligations. Lenders are not being permitted to declare the arrearages accruing during the forbearance period to be immediately due upon loan payment resumption. Further, the CARES Act provided for a moratorium against foreclosures and evictions that, when combined with the Centers for Disease Control and various localities' foreclosure and eviction moratoriums, resulted in nearly all foreclosures and evictions being halted nationwide during 2021. As foreclosures resume, there will be attendant foreclosure-related litigation, accordingly.

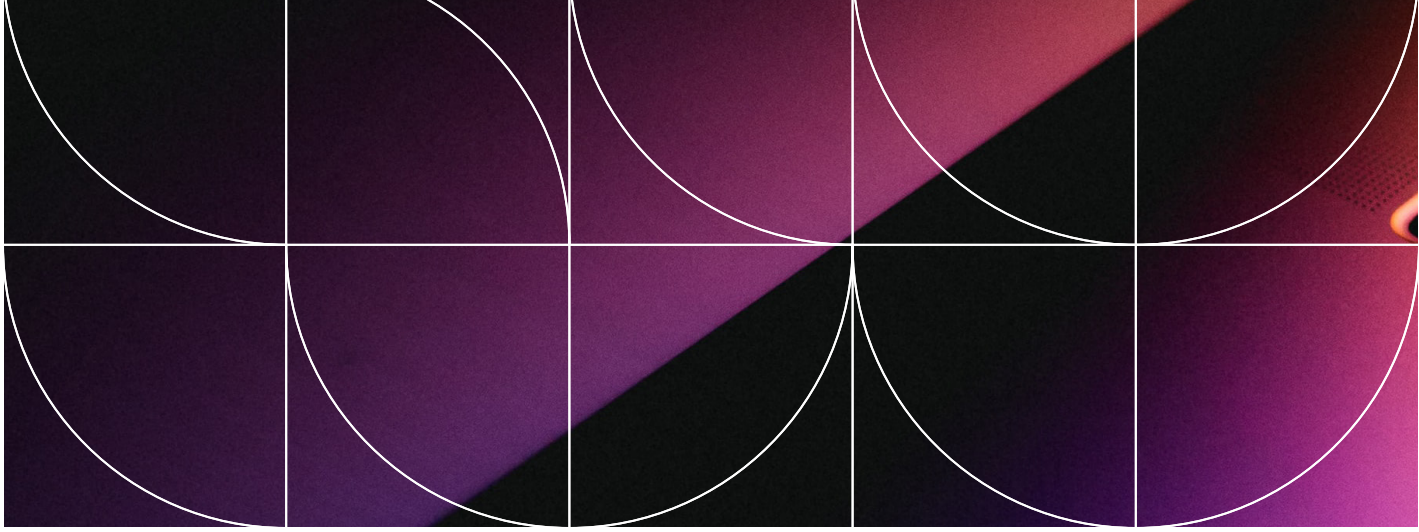
The CARES Act further placed special requirements on companies that report payment information to consumer credit reporting agencies which have resulted in many borrowers being reported as current on their loans even though they are not paying because their loans are in forbearance. Meanwhile, mortgage interest rates hit an all-time low of 2.65% for 30-year mortgages during the week ending January 7, 2021, keeping loan costs low. Interest rates remained at historic lows throughout 2021, while property values skyrocketed. While interest rates are expected to rise in 2022, still relatively low rates coupled with high property values will continue to permit many property owners to refinance or sell their way out of their problem debts in 2022, rather than have to try to litigate their way out of them. But for those mortgage loans which were either already in material default before the onset of the COVID-19 emergency relief, or which fall out of forbearance still in material default, foreclosures and evictions will resume or be commenced in 2022.

Further, during the COVID-19 pandemic, all federal student loan payment obligations (92% of all student loans; roughly $1.59 trillion) have been paused. The current administration has extended the student loan pause through (at least) May 1, 2022. During the pause, federal student loans have no payment obligations, incur no new interest or late penalties, and all collection actions on defaulted federal student loans are stopped. The Education Department granted and extended flexibility to student loan services to assist borrowers who do not qualify for the automatic relief. Many private lenders have implemented forbearance options that have allowed borrowers to postpone their monthly payments and provided for reduced payment options and other relief. There has been a shortage of student loan private civil litigation during the COVID-19 pandemic as a result. For those students whose loans do not end up being cancelled, when the federal or private student loan pauses end, if they are unable to afford the monthly payments, they can apply for hardship relief, so this trend is expected to continue throughout much if not all of 2022.

FinTech

Consumers are increasingly demanding new and emerging financial products and services from both traditional and non-traditional lenders. FinTech, new technology that seeks to improve and automate the delivery and use of financial products and services, is expected to be the subject of particular emphasis in 2022, both in consumer and government enforcement litigation.

New and novel lending products and services tend to suffer systemic attacks in their infancies, and non-bank lenders that lack a financial regulator may be more likely to miss or misapprehend the myriad, byzantine regulatory and compliance requirements that exist at the federal, state, and even local levels. We predict that in 2022 there will be an increased focus by civil plaintiffs and government agencies alike on FinTech products and services.



Key Trends in Commercial Litigation

eDiscovery Litigation

— By Jay Carle and Ryan Tilot

Business collaboration platforms are changing the way companies conduct business, and they are also changing the way discovery is conducted in litigation.

For example, Microsoft estimates that Teams—one of the most popular collaboration platforms used by businesses—currently has 145 million daily active users. These users are creating and storing data that may be potentially relevant to litigation.

Over the past few years, companies have steadily adopted the use of online collaboration platforms and instant messaging communications to conduct business. For some, use of these tools has already surpassed email as the primary internal business communication and collaboration platform. Millions of users each day use collaboration platforms to communicate in real time, share and edit documents, record video calls, and conduct web-based presentations. The COVID-19 pandemic and the necessity to keep workforces connected while working almost exclusively from home has rapidly increased the adoption of these tools and gave this transition a shot of adrenaline. For example, Microsoft estimates that daily active users of Microsoft Teams—one of many collaboration platforms in the market—has skyrocketed from 13 million active daily users in 2019 to 145 million active daily users in 2021. Collaboration platforms are now the second most common form of communication in business, behind email.

Accordingly, we expect to see a steady increase in disputes surrounding the discoverability of certain data residing in collaboration platforms. For example, the court in *Benebone LLC v. Pet Qwerks, Inc.,* et al., WL 831025, at 3 (C.D. Cal. 2021) ordered plaintiff to review and produce messages from its collaboration platform, making the request comparable to the search and production of email. On the other hand, the court denied plaintiffs' request for such messages in *Laub v. Horbaczewski,* WL 7978227 at 5-6 (C.D. Cal. 2020), concluding that plaintiffs' request was largely speculative that a search of chat messages within the collaboration platform would identify additional responsive messages. The court reasoned that the request was not proportional to the needs of the case. In summary, courts are more frequently weighing in on the discovery of data created and stored in collaboration platforms and their focus is on whether data from collaboration platforms is relevant and proportional to the needs of the case.

The problems law departments are facing, and will continue to face with increasing regularity, from a legal compliance and litigation discovery perspective are two-fold. The first issue involves how collaboration platforms are architected and the way in which data is stored. Many collaboration platforms are developed with the end user in mind, with far less emphasis on the importance of identification, preservation, and search of electronically stored information for litigation. For example, some collaboration platforms store chats in one location and documents shared during the chat in a completely different location with no way to collect them in a cohesive, linked fashion. The documents shared during the chat may only be stored and associated with the user that sent the chat but not the other users who received the shared document. Accordingly, it is plain to see that where data is stored and who it is associated with creates issues when businesses need to preserve and collect information from particular users. Placing a legal hold on a particular individual may not preserve all relevant parts of a chat thread nor the documents that were exchanged during the chat communication.

In addition, the format in which data is stored is also problematic. Many collaboration platforms store chats as individual messages and do not link messages together. This makes it difficult from a preservation, search, and collection standpoint as businesses face difficulties with identifying relevant information and messages. Similarly, large discussions within collaboration platforms that involve many users known as "channels" oftentimes store data in locations that are not associated with any user involved in the channel. Various third- party tools are beginning to appear on the market to better handle the preservation and collection of information in collaboration platforms, but those, too, have developmental progress to make in order to simply catch up, not to mention staying current with the rapid development of new features and functionality within collaboration platforms. All of these challenges, among others, can make it difficult for businesses to comply with their legal hold and discovery obligations.

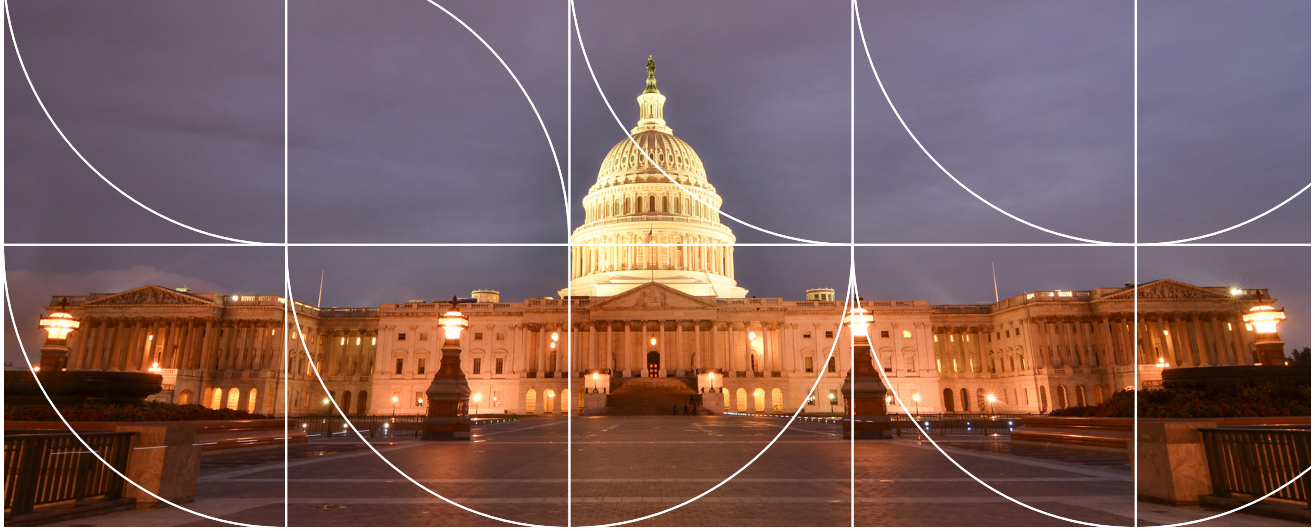
Our attorneys and technologists work hand-in-hand with corporate legal departments and IT organizations to address the inherent challenges associated with collaboration platforms.

These issues are exacerbated by the fact that some businesses had to rapidly onboard and expand their use of collaboration platforms at the outset of the pandemic with little planning to accommodate a remote workforce. In the rush, some law departments may not have been consulted or did not have the time and resources to monitor data retention and legal hold policies and procedures during these quick implementations. Even law departments that are consulted on retention and preservation practices involving collaboration platforms struggle to implement effective policies and procedures because of the inherent architecture issues previously discussed.

We expect these challenges will continue as the discovery from collaboration platforms becomes commonplace. Both in-house and outside counsel need to be aware of these inherent issues, and upfront processes and procedures need to be in place to address preservation and collection issues. Now that businesses have had a chance to recover from the initial impact of the pandemic, law firms and eDiscovery vendors are working with law departments and IT organizations to address these issues. Architecting solutions and resolving information governance, records and information management, and eDiscovery readiness issues as they relate to collaboration platforms. Some law departments are electing to adopt third-party solutions to address preservation and collection gaps that cannot be resolved by the collaboration platforms.

Our attorneys and technologists work hand-in-hand with corporate legal departments and IT organizations to address the inherent challenges associated with collaboration platforms.

At Seyfarth, we are actively working with our clients to address issues raised by collaboration platforms from an eDiscovery and information governance perspective. Our attorneys and technologists work hand-in-hand with corporate legal departments and IT organizations to address the inherent challenges associated with collaboration platforms. We also work with trusted eDiscovery vendors who have spent years developing tools and processes that can help fill preservation and collection gaps. The workplace is evolving and the way in which companies are conducting day-to-day business post-pandemic will almost certainly require organizations to continue to use collaboration platforms to conduct business, making it more likely that information exchanged on such platforms is relevant to litigation or a legal investigation.



Key Trends in Commercial Litigation

Fair Credit Reporting Act

— By Esther Slater McDonald

In the last decade, the number of lawsuits filed under the Fair Credit Reporting Act (FCRA) has increased year over year, and we expect that trend to continue in 2022.

In addition, we expect to see an increase in investigations and enforcement actions by the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC), with an emphasis on imposing equity, obtaining monetary relief, and expanding agency authority.

Regulatory oversight

Under the Biden Administration, the CFPB and FTC have had a marked transformation and have not been shy in signaling their intent to engage in robust supervision and enforcement, beyond what we have seen before. In the fall of 2021, the CFPB issued a report on consumer credit disputes and guidance on name-only matching procedures. In both documents, the CFPB focused on the alleged disparate impact that reporting errors have on minorities and communities of color. In press releases, the CFPB vowed to investigate the root causes of racial and demographic disparities and broadly outlined the agency's enforcement agenda. On the latter, the CFPB stated that it will seek civil penalties and compensation for victims will closely collaborate with the FTC to expand oversight of consumer reporting agencies (CRAs) and to bring "Big Tech giants" and other "data brokers" under the FCRA's purview and will refer matters to other agencies when the CFPB believes that business practices may violate anti-discrimination laws.

Similarly, the FTC has outlined its "vision and priorities" to include a focus on harm to marginalized communities and has confirmed its intention to use all tools and authorities, including rulemaking, for enforcement. Time will tell whether such measures will include an effort to find other means to obtain monetary recovery from businesses in light of the US Supreme Court's holding that the FTC cannot pursue restitution or disgorgement under Section 13(b) of the FTC Act.

These statements indicate that the CFPB and FTC plan to aggressively challenge existing policies and practices of credit bureaus, background screening companies, and other companies engaged in data collection and transfer and will seek to broaden the reach of the FCRA and the FTC Act through creative legal theories.

Policies and procedures

Matching. CRAs continue to refine their policies and procedures to promote accuracy in matching. Typically, CRAs aim to include in a consumer report only those records or accounts that belong to the consumer, but that goal must be balanced against avoiding underreporting. Overly strict matching procedures can lead to reports that fail to include records or accounts belonging to a consumer. Concerns about underreporting have increased as courts have limited the personal identifiers available in public records.

Recently, the Eleventh Circuit offered a solution to underreporting by holding that it was accurate for a CRA to report a public record based on a name-only match without confirming the record belongs to the consumer, where the CRA instructed the user of the report that additional investigation was needed to determine whether the record belonged to the consumer. *Erickson v. First Advantage Background Servs. Corp.,* 981 F.3d 1246, 1253 (11th Cir. 2020). Notably, the CFPB ignored the Eleventh Circuit's holding

when the agency opined that CRAs "that use name-only matching violate [the] FCRA." Advisory Opinion, 12 CFR Part 1022 at 14. CRAs considering name-only matching should be aware of the CFPB's unbending opposition to the practice.

To promote accuracy in matching, CRAs have been implementing and regularly updating common names policies whereby CRAs identify common name combinations and require an additional identifier(s) to match a record to that name. Although there is no legal or industry standard for defining common names, CRAs developing common names lists often consider census data and internal reporting records and examine national trends and geographic subsets. In 2022, we expect to see continued litigation and regulatory investigations about matching procedures, particularly as agencies probe the impact that matching procedures have on minorities. *See* Letter from Seven US Senators to the CFPB (Nov. 10, 2021).

Credit Reporting. In the credit space, we anticipate increased litigation and investigation in various areas, including the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), bankruptcy filings, and contractual disputes. Throughout the pandemic, financial institutions have offered numerous arrangements, including loan forbearance and modifications, to consumers to accommodate economic difficulties. In 2020, the CARES Act amended the FCRA to provide that, if a creditor provides an "accommodation"to a debtor, the creditor (if it reports data to a CRA) must either "report the credit obligation or account as current" or, if an account was delinquent at the time of the accommodation, "maintain the delinquent status" during the accommodation period. 15 U.S.C. § 1681s-2(a)(1)(F)(ii)(I)–(II). Since then, consumers have filed numerous lawsuits against creditors and bureaus, alleging that they are inaccurately reporting accounts subject to accommodations. Defendants have often prevailed by showing that the derogatory reporting accurately reported a delinquency occurring *before* the accommodation. *See, e.g., Porter v. Experian Info. Servs., Inc.,* No. 121CV00453SDGRGV, 2021 WL 5068262, at *9 (N.D. Ga. Oct. 30, 2021); *Hafez v. Equifax Info. Servs., LLC,* No. CV209019SDWLDW, 2021 WL 1589459, at *5 (D.N.J. Apr. 23, 2021). To minimize risk, creditors should document payment accommodations and have collections and disputes teams coordinate to ensure that payment accommodations are properly being reported.

As payment accommodations expire, bankruptcy filings may rise, and, with that, claims regarding the reporting of accounts in bankruptcy. We anticipate that lenders, servicers, and bureaus will face claims of inaccurate reporting of accounts pending and discharged in bankruptcy. The plaintiffs' bar continues to come up with new theories of liability, including claims relating to historical account information, payment history during a pending bankruptcy, and the legal effect of a discharge.

Those novel theories of liability extend beyond bankruptcy to contracts. The plaintiffs' bar continues to push the theory that accuracy includes factual determinations and legal conclusions. Thus, the theory goes, the FCRA's requirement of reasonable procedures to ensure maximum possible accuracy requires credit bureaus to determine not only whether a consumer opened an account but also whether the underlying contract is legally enforceable. In July 2021, the Seventh Circuit rejected this theory, holding that accuracy is limited to factual determinations and does not include legal judgments. *Chuluunbat v. Experian Info. Sols., Inc.,* 4 F.4th 562, 569 (7th Cir. 2021); *see also Losch v. Nationstar Mortg. LLC,* 995 F.3d 937, 946 (11th Cir. 2021). Whether credit bureaus must arbitrate legal disputes between consumers and creditors will be an ongoing topic of litigation in 2022.

Liability and damages

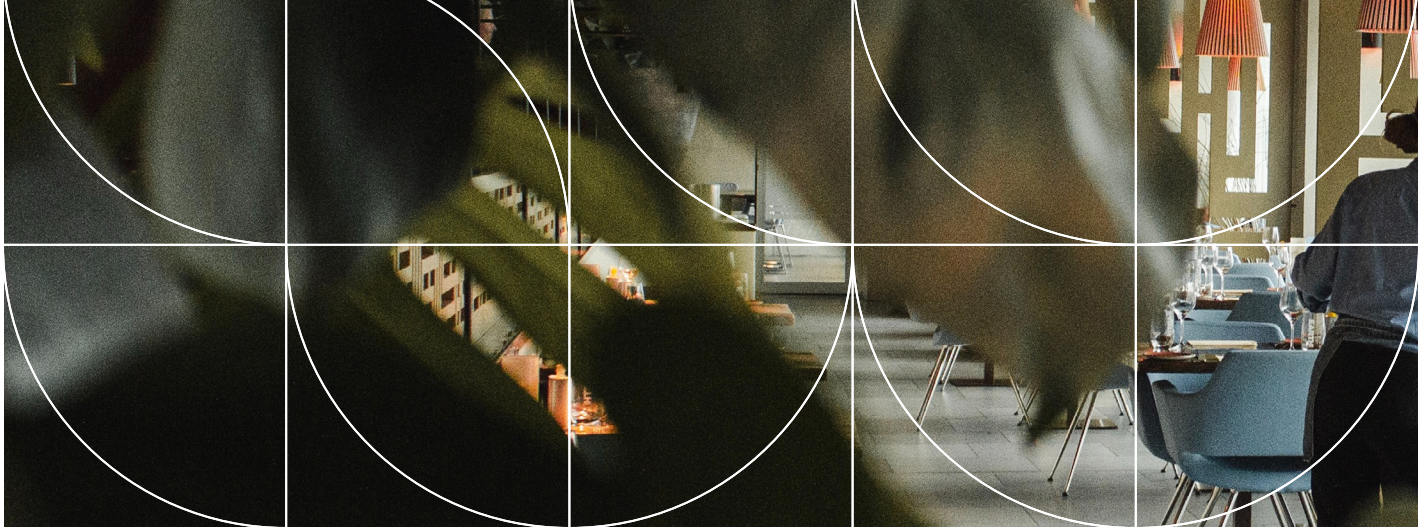
Standing. In June 2021, in Trans Union LLC v. Ramirez, the Supreme Court reiterated that only consumers who were concretely harmed by an alleged FCRA violation have standing to sue. 141 S. Ct. 2190, 2200 (2021). The Court held that consumers suing a credit bureau over inaccurate information in internal credit files that had not been published to third parties did not have standing to sue for damages. Id. The Court rejected the plaintiffs' argument that the risk of publication created a concrete injury. Id. at 2210. Since then, defendants have raised Ramirez to challenge similar claims of harm in cases not involving publication of the disputed information. Because most challenges have been facial, district court rulings applying Ramirez have typically turned on whether a complaint alleges dissemination.

As cases progress, however, defendants are likely to raise factual challenges to standing based on proof of non-publication. And, even where concrete harm exists, defendants may challenge whether that injury is sufficient to establish actual damages for negligence claims. *See, e.g., Kundmueller v. Pentagon Fed. Credit Union,* No. 520CV00056KDBDSC, 2021 WL 4806733, at *4 (W.D.N.C. Oct. 14, 2021).

Willfulness. In 2021, the Second and Seventh Circuits joined the Third and Eleventh Circuits in holding that subjective intent is irrelevant to willfulness.

In Safeco Insurance Company of America v. Burr, the Supreme Court held that, although willfulness includes reckless disregard of the law, a company does not willfully violate the FCRA if the company's "reading of the statute … was not objectively unreasonable." 551 U.S. 47, 69 (2007). Since then, the plaintiffs' bar has argued that Safeco requires a defendant to show that it actually adopted and applied an objectively reasonable interpretation of the law. Although some district courts continue to accept this argument, circuit courts have rejected it when presented with the issue.

Given the circuit courts' growing consensus on this issue, defendants are likely to have more success in obtaining dismissals of or summary judgment on willfulness claims. However, because class liability and punitive damages generally turn on willfulness, companies should expect consumers to continue to litigate the issue.



Key Trends in Commercial Litigation

Franchise and Distribution

— By John Skelton and Alison Eggers

Recent economic and social forces have highlighted rising challenges to traditional franchisor and franchisee relationships. Here are three trends and developments to watch in the coming year.

Employee misclassification suits likely to spread, and franchisors are fighting back

The misclassification of employees as independent contractors has been a significant issue and risk for employers for years. More recently, franchise relationships have been the target of misclassification challenges which have taken on even more significance after passage of California's "AB5." The legislation, which codified the California's Supreme Court's ruling in *Dynamex Operations W. v. Super. Ct.,* 4 Cal. 5th 903 (2018), presumptively extended employee status to all workers who perform services for a company unless the company can meet a three-prong "ABC test." While the intent of AB5, as stated by the legislators behind it (among others), was primarily focused on the alleged misuse of independent contractors (so called gig economy workers) in the ride-sharing and food delivery industries, as drafted, a literal application of the ABC test would make franchisees employees. With "employee misclassification" litigation, especially in California, increasingly targeting the franchisor/franchisee relationship the International Franchise Association has sued the State of California seeking a declaration that AB5 and the ABC test should not apply to franchising. Especially for franchise models focused on owner-operators, we expect more franchisees dissatisfied with their franchise relationship to use misclassification tests to claim employee status.

Employee misclassification cases are particularly challenging in the context of a franchise relationship. For example, there is an inherent conflict between Prong A of the "ABC test"—which requires that for a worker to be properly classified as an independent contractor, that worker must be free from control—and the franchise relationship—which actually *requires* control. Indeed, the FTC Franchise Rule defines a franchise as a "continuing commercial relationship or arrangement" in which it is agreed that, among other things, the "franchisor will exert or has authority to exert a *significant degree of control* over the franchisee's method of operation, or provide significant assistance in the franchisee's method of operation." *See* 16 C.F.R. § 436.1(h) (emphasis added).

These cases, and others, are "bet the company" cases not only for individual franchisors, but for the franchise business model itself. Franchised businesses are governed by franchise agreements, nearly all of which specify that the franchisee is an independent contractor operating an independent business. Franchisor control is a fundamental element of a valid franchise relationship and is necessary to protect the brand and provide uniformity throughout the network. Even if eliminating control were possible (it is not), ABC tests still present a significant problem for franchisors. For example, Prong B requires an entity to demonstrate that the services performed are "outside the usual course of the business of the employer" while Prong C requires that the individual be engaged in an "independently-established trade." If applied literally and without regard to the nature and structure of a valid franchise relationship, both carry uncertainty and risk for franchisors. Given the significant damages which can arise in a misclassification claim, we expect these challenges to continue.

Stepping back from brick and mortar
Among the shifting business impacts in franchising caused by COVID-19 is the emergence of, and evolution to, non-traditional franchise models that do not rely on—or even require—"brick and mortar" business locations. While franchise models that operate out of a franchisee's home, vehicle, or rented office or warehouse space may offer lower start-up costs and more attractive flexibility to franchisees, they also create a variety of unique challenges for franchisors.

One such challenge is the collection of financial and operational data traditionally collected through integrated "point of sale" systems and used by franchisors to understand real time performance, to assess franchisees' compliance with provisions of the franchise agreement, and to prepare mandated franchise disclosures. All of this will be particularly important in the near term for the preparation of accurate franchise disclosure documents because regulatory scrutiny of financial performance representations remains at a historical high.

Joint employer and misclassification challenges are also likely to be heightened in non-brick and mortar franchisees. Franchisees that are leanly staffed, sometimes by a single individual, may be less sophisticated and more challenged to shoulder the comparably heavier financial and operational burdens of brick and mortar franchises. As a result, these franchisees may seek greater guidance by franchisors which, as discussed above, could be seen as improper control implicating the ABC test. The unique challenges of these evolving models require careful navigation by franchisors.

Managing social media
Social media is an integral part of today's economy. Franchising, as a business model, inherently incorporates a significant degree of autonomy on the part of franchisees. Balancing that autonomy with a franchisor's interest in protecting its reputation and brand in the public eye requires careful attention to the social media activities of franchisees and, at times, swift responses to missteps and statements that do not align with franchisor values. Trending negative publicity risks damage not only to the source franchisee, but to the franchisor, the systems as a whole, and, by extension, other franchisees. The damage can be difficult and costly to repair.

Some franchise systems have turned to social media policies in an effort to minimize the potential for fallout from poorly-received or controversial social media messaging by franchisees. We urge franchise systems to develop and implement such policies cautiously. Social media policies may have the benefit of standardizing brand and image messaging to the public and, in some cases, reserving to the franchisor messaging on potentially sensitive topics. The risk, however, is that social media policies may be used as evidence of an impermissible degree of control by the franchisor over franchisee operations. They may also invite constitutional challenges, discrimination claims, or their own public relations challenges if policies are perceived to unfairly affect employees based on a protected class.

Franchisor control is a fundamental element of a valid franchise relationship and is necessary to protect the brand and provide uniformity throughout the network.

Putting a Premium on Cyber Insurance in 2022

— By Thomas Locke

Almost every entity will face two important insurance issues in the upcoming year: rising premiums and cyber/data-breach coverage.

The upcoming year will see litigation on many important insurance issues, including: whether brokers breached their duties to obtain appropriate coverage, insurance for climate change, coverage disputes in sexual molestation litigation, asbestos bankruptcy coverage litigation, the status of additional insureds under a variety of policies, representation and warranties coverage claims, potential coverage for anti-trust claims, and whether coverage exists for COVID-19 related losses. This section will focus on two issues almost every entity will face in 2022: rising premiums and cyber/data-breach coverage.

Rising insurance premiums
2021 was a "hard" insurance market, with substantial premium increases in most areas. 2022 should see some moderation in premium increases, with the notable exception of premiums for cyber, employment practices liability, errors and omissions coverage, and property policies in fire and storm-prone regions.

In November 2021, Willis Towers Watson estimated that property insurance rate increases will rise "only" 2 to 10 percent as compared to 2021, which saw increases up to 25 percent. That likely will not be the case in the southeast and far west, which have seen higher than normal catastrophic losses. General liability premiums are estimated to increase 5 to 12.5 percent as compared to 2021, which saw increases up to 15 percent. Notwithstanding more litigation in 2021, increased insurance capacity and insurer competition has moderated premium increases, particularly in connection with umbrella and excess liability policies.

Directors and officers (D&O) premium increases are expected to be relatively modest, with the exception of initial public offerings, special purpose acquisitions companies, oil and gas, health care and higher education entities, which may see increases as high as 25 percent. Employment practices liability premium increases are estimated to be as large as they were in 2021, 10 to 30 percent. Errors and omissions premium increases for accountants, consultants and law firms are estimated to be in the 10 to 20 percent range. Premium increases also have been fueled by low interest rates through most of 2021 and claims relating to vaccine mandates, sexual harassment and gender discrimination litigation, and privacy litigation.

Increases should be lower for policyholders with favorable claim histories. Policyholders may attempt to mitigate premium escalation by increasing the self-insurance component of their risk management program. Of course, increasing, for example, self-insured retentions, enlarges the policyholder's risk and, perhaps, the risk for business partners who may rely on the policyholder's insurance, particularly as additional insureds.

Cyber and data-breach insurance issues
Cyber and data-breach insurance present unique issues. Since 2019, the US has seen a 400 percent increase in ransomware events. As a result, cyber insurance premiums are expected to jump by 50 to 150 percent on top of 10 to 30 percent increases in 2021. Health care, higher education, financial companies, construction, media, and technology entities probably will experience the most significant premium increases.

In addition, insurers likely will reduce their cyber insurance risk by adding exclusions, increasing self-insured retentions, decreasing sublimits for certain kinds of losses, and reducing the time period for business interruption and other time element loss. And, insurers will seek to control expenses by limiting who policyholders can retain as ransomware experts, accountants and attorneys. Insurers will include new requirements for early notice, detailed documentation of damages, and strict insurer consent prior to incurring costs, even though ransomware events require rapid responses. In short, in 2022, underwriting cyber insurance coverage and claim handling will be even more challenging than in 2021.

... insurers likely will reduce their cyber insurance risk by adding exclusions, increasing self-insured retentions, decreasing sublimits for certain kinds of losses, and reducing the time period for business interruption and other time element loss.

Insurance coverage for cyber breaches involves multiple types of losses. Two broad categories are first-party losses and liability to third parties. The first category involves loss that the policyholder itself has incurred, e.g., damage to computer systems, loss of the policyholder's data, loss of income. The second category involves liability that the policyholder may have to its customers and business partners, *e.g.,* for loss of their data.

Cyber first-party insurance issues
Cyber insurance policies often cover first party losses like ransom for cyber extortion, restoration of data and loss of hardware and software. Cyber policies also may provide coverage for interruption of business operations after a denial-of-service attack and regulatory investigation costs.

In the event that an entity lacks a cyber insurance policy, for now, the entity may be able to turn to other policies for partial first-party coverage for ransomware attacks. For example, kidnap and ransom or specialty crime policies or coverage parts may provide reimbursement for the cost of the ransom. Historically, insurers who issued kidnap and ransom policies provided coverage for the ransom payments associated with cyberattacks. In 2022, policyholders should expect that kidnap and ransom policies will exclude that coverage. Insurers may argue that payment of ransom with Bitcoin violates the exclusion regarding willful or deliberate violation of the law. And, insurers may argue that the act of war exclusion applies to cyberattacks originating from Russia, China, and North Korea. Lloyd's Market Association recently offered four clauses to exclude coverage for war from cyber insurance policies. The clauses offer increasingly restrictive for cyber operations, including the possibility of excluding coverage for losses resulting from retaliation between China, France, Germany, Japan, Russia, United Kingdom, or United States, and/or losses having a major detrimental impact on a state's security or essential services.

In summary, 2022 will be a challenging year for entities seeking to renew cyber insurance policies and to obtain coverage for first-party and liability cyber-related losses.

Crime or computer fraud insurance may also be an avenue to obtain coverage for cyberattacks. In March 2021, the Indiana Supreme Court held that a policyholder may be entitled to coverage under a crime policy's "computer fraud" provision for ransom payments. *G&G Oil Co. of Indiana, Inc. v. Continental Western Ins. Co.,* 2021 Ind. LEXIS 182 (Ind. Mar. 18, 2021). But, the court warned that not every cyberattack may be fraudulent. This is particularly true where an attacker easily accessed the policyholder's computer system because there was insufficient security in place. In 2022, expect insurers to include in crime and computer fraud policies exclusions for ransom paid in connection with cyberattacks. Similar coverage issues arise when an employee is tricked into transferring funds by wire to an imposter. It is unclear whether, in the future, insurers will broadly exclude from crime and computer fraud policies coverage for fraudulent wire transfers.

In the short term, one potential source of coverage for hardware and software loss may be property insurance policies. In November 2021, an Ohio appellate court held that coverage could exist for a ransomware attack under a property policy. *EMOI Serv., LLC, v. Owners Ins. Co.,* No. 29128 (Ohio Ct. App., Nov. 5, 2021). The court reasoned that the loss of use of the computer system could be property damage. Insurers argue that property policies do not cover ransomware attacks because there is no physical damage to property. That argument has been very successful for insurers in the context of pandemic coverage litigation. However, with respect to the "media" coverage language at issue in the Ohio case, the court reasoned that the policy did not require "tangible" physical damage.

A 2020 Maryland federal court decision, *National Ink & Stitch LLC v. State Auto Property & Casualty Insurance Co.,* 435 F. Supp. 3d 679, 680 (D. Md. 2020), similarly held that coverage for the cost to replace computer systems caused by a ransomware attack existed under a property policy. That policy defined covered property to include data and software. The court rejected the argument that the computers were still functional. The court reasoned that the computer system was slower, and the policy did not require that the system be completely and permanently inoperable.

Whether ransom, crime, property, and other non-cyber policies cover ransomware attacks will continue to be litigated throughout 2022. Policyholders should anticipate that, in 2022, insurers will add broad cyber exclusions to non-cyber policies.

Cyber liability insurance coverage issues

Ransomware attacks, data breaches, and other cyber issues may result in liability to third parties. An obvious situation is when a cyberattack results in the disclosure of confidential financial or biometric information. This type of disclosure has occurred with respect to health care providers and insurers, financial institutions, retailers, professional services providers, social media companies, and just about every other entity that maintains a database with the confidential information of third parties. Cyber insurance is broadly designed to cover this liability. However, as discussed above, in addition to substantially increasing premiums, cyber insurers are reducing their risk by lowering sublimits, increasing self-insured retentions, reducing the time period for business interruption and other time element loss, and adding exclusions for high risk area. At renewal, policyholders should carefully review their cyber risks and practices and analyze every changed coverage provision.

One area that is often overlooked is the cost of notifying consumers and other third parties of a data breach. That cost can be substantial and should be incorporated into a comprehensive cyber policy. Policyholders also should review carefully proposed terms regarding retention of experts, accountants, and attorneys. Policyholders want control of communications with customers. Insurers may seek control in order to reduce costs. Policyholders should weigh the cost-benefit of ceding control.

In 2022, expect to see coverage litigation regarding new cyber liability issues. For example, in October 2021, the US Department of Justice threatened to use the False Claims Act (FCA) to pursue contractors who fail to comply with cybersecurity requirements. Cyber and D&O policies may provide coverage for defense costs and settlements. *See generally Astellas US Holdings Inc. v. Starr Indem. & Liab. Co.,* No. 17-cv-08220 (N.D. Ill. Oct. 8, 2021). However, in the

future, expect insurers to rely on exclusions for claims brought by or on behalf of local, state, federal, or foreign governments to preclude coverage for FCA claims and relators' qui tam actions. Insureds can reduce their risk by requiring that renewal policies narrow the applicability of certain exclusions. For example, "willful act" language should include a "severability" provision stating that the exclusion applies only to the director or officer who commits the act and not to other insureds. And, exclusions relating to fraud and willful acts should apply only when a final adjudication has established that the precluded act occurred. "Insured versus insured" provisions should include whistleblower exceptions.

In 2022, expect more coverage litigation regarding Illinois' Biometric Information Privacy Act (BIPA), which is discussed in the class action section of this publication, and similar state laws. So far, coverage decisions have been mixed. These decisions highlight coverage issues that may arise in connection with California, Virginia, and Colorado's privacy statutes requiring greater consumer control over personal information. (Massachusetts, New York, Florida, Washington, Pennsylvania, Ohio, New Jersey and Minnesota are considering similar or broader legislation, including private rights of action.)

In summary, 2022 will be a challenging year for entities seeking to renew cyber insurance policies and to obtain coverage for first-party and liability cyber-related losses. Premiums will increase, sublimits will decrease, exclusions will narrow coverage, documentation requirements will be added. Insurers will seek to limit coverage for response costs associated with cyber and data breaches. Policyholders can protect themselves by implementing best practices to reduce the likelihood of attacks and by responding quickly and thoroughly to breaches, including working with insurers to mitigate and document loss and potential liability. Policyholders may also need to explore property, crime, ransom, general liability, D&O, errors & omissions and other policies to obtain additional coverage for data breaches and cyber-related losses.

Key Trends in Commercial Litigation

Health Care Litigation

— By Jesse Coleman and Owen Wolfe

With the COVID-19 pandemic continuing to fuel health care-related litigation, we can expect the surge of health care litigation to continue in 2022, addressing false claims, privacy issues, and vaccine-related issues.

False Claims Act (FCA) investigations and litigation will be a key driver of health care litigation through 2022. After a relative down year in fiscal year 2020, when the US Department of Justice (DOJ) reported recoveries from FCA investigations and litigation of only $2.2 billion, the DOJ's recoveries in fiscal year 2021 and after exploded far beyond that figure. The first quarter of fiscal year 2021 alone saw FCA recoveries of $3.23 billion, driven in large part by a massive settlement with a large pharmaceutical company and its shareholders. Although recoveries quieted down in the spring and early summer, by mid-summer and fall 2021, massive recoveries continued to come in, including after the close of the fiscal year. From July 2021 through mid-November 2021, the DOJ announced settlements in excess of $931 million and convictions or guilty pleas in excess of $765 million. The recoveries included a $447.2 million settlement right after the close of the fiscal year in early October 2021.

We expect that large recoveries will continue into 2022, in part because in late 2021, the DOJ announced FCA indictments seeking recovery of billions of dollars, including one indictment for $1.4 billion. The indictments and recoveries include FCA claims relating to Paycheck Protection Program (PPP) loans, which will likely continue to be a source of FCA claims into 2022.

Indeed, given the 2021 filings, the ongoing pandemic, and the government's plans to pump even more funds into the economy, we can anticipate that 2022 will again exceed the down year of 2020 and include an ever-growing number of FCA filings by the government and *qui tam* relators. For companies in the health care industry who obtain reimbursement from the government, these numbers indicate that they can expect more government scrutiny and possible whistleblower claims.

Another important aspect of health care-related litigation during the pandemic has been in the area of health care-related privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA). In 2021, the US Office of Civil Rights announced settlements of HIPAA-related investigations and claims totaling in the hundreds of thousands of dollars, including numerous settlements of claims under the HIPAA Right of Access Initiative regarding patients' ability to access their health records under HIPAA. We anticipate that HIPAA- related claims will continue to increase as a result of increased use of telehealth and corresponding HIPAA violations and fraudulent activity seeking to compromise or access private information.

HIPAA is only part of the story, however. As detailed in the 50-State Survey of Health Care Information Privacy Laws compiled by Seyfarth's Health Care, Life Sciences & Pharmaceuticals group, the battleground in health care information privacy litigation is often in state courts involving state laws that are more restrictive than HIPAA. For example, as shown in the survey, Texas' state privacy law covers not just health care organizations but anyone who comes into possession of personal health care information. Tex. Health & Safety Code Ann. § 181.001(b)(2); Tex. Ins. Code Ann. § 602.001(1). Violations can trigger fines of anywhere from $2,000 to $50,000 per violation. Tex. Bus. & Com. Code Ann. § 521.151(a). Many other states have similarly broad laws.

It is critical that companies be aware of, and comply with, not only HIPAA, but any applicable state laws as well. If you have questions about the application of state privacy laws to your business, you should review the survey and contact a Seyfarth Health Care, Life Sciences & Pharmaceuticals attorney for more information.

Finally, some of the highest profile health care litigation in 2021 has related to vaccination requirements imposed on health care workers and others by federal, state, and local governments, as well as by private employers. Among other things, health care workers in New York and Maine mounted challenges to those states' respective rules requiring all health care workers to be vaccinated, only to have those challenges rejected at the injunction stage by two different federal appeals courts. The US Supreme Court also declined to enjoin the Maine and New York vaccination rules pending further appeal.

We expect that large recoveries will continue into 2022, in part because in late 2021, the DOJ announced FCA indictments seeking recovery of billions of dollars, including one indictment for $1.4 billion.

Numerous private health care employers have been hit with lawsuits as well, and a few examples illustrate the coast-to-coast nature of these lawsuits. In Illinois, a health care employer has been engaged in litigation with plaintiffs proceeding under pseudonyms, who have invoked a unique Illinois Health Care Right of Conscience (HCRCA) statute to support their claims. In response to this and similar lawsuits, the Illinois legislature amended the HCRCA to exclude COVID-19 vaccination from its scope, but the amendment will not go into effect until sometime in 2022, likely leading to more litigation in the interim. In Massachusetts, a prominent hospital defeated a preliminary injunction motion from employees threatened with termination due to their refusal to comply with the hospital's vaccination requirements, which the employees subsequently appealed. The First Circuit Court of Appeals and the US Supreme Court both denied the employees' applications for an injunction pending appeal, but the case remains pending. In California, a health care consortium with national reach was similarly sued by a group of employees whose motion for a preliminary injunction was denied. The employees subsequently dismissed the case, without prejudice, and may re-file in another jurisdiction.

This litigation is happening against the backdrop of federal regulations requiring certain employers to require COVID-19 vaccinations for their employees. Most relevant to the health care industry, the Centers for Medicare & Medicaid Services (CMS) issued a rule on November 5, 2021, requiring vaccination for staff associated with any facility regulated by Medicare conditions of participation or conditions of coverage. The CMS rule includes a requirement that covered facilities allow for exemptions to staff with recognized medical conditions or religious beliefs, observances, or practices. The rule was quickly challenged in court, including in a suit filed by ten states (Missouri, Nebraska, Arkansas, Kansas, Iowa, Wyoming, Alaska, South Dakota, North Dakota, and New Hampshire) in Missouri federal court. The Missouri court and a federal court in Louisiana subsequently issued orders enjoining the implementation and enforcement of the CMS rule, but appeals from those orders and other litigations involving the CMS rule remain pending.

Litigation over the CMS rule is likely to continue into 2022. If the rule does survive, it will likely spawn litigation over what constitutes appropriate accommodations based upon medical conditions or religious beliefs. It may also lead to litigation over whether the federal rule preempts states rules prohibiting employee vaccination requirements, like Montana and Texas, or other laws that plaintiffs assert prohibit vaccine requirements, such as the Illinois HCRCA discussed above.

Key Trends in Commercial Litigation

International Dispute Resolution

— By Sara Beiro Farabow and Talat Ansari

Increased international arbitration activity is likely to continue during 2022. Much of this increase is due to the disruption that COVID-19 continues to bring to international business and supply chains.

2021 was a mixed year for international dispute resolution (IDR) globally. While the number of decided IDR cases increased in some jurisdictions, in others, they went down because of restrictions imposed by different countries due to COVID-19. The majority of IDR cases are decided either by arbitration or by alternate dispute resolution (ADR) procedures. This section focuses on such resolutions.

The American Arbitration Association (AAA) continues to be the largest institution in the world for arbitral proceedings. International arbitrations are handled by the AAA's International Center for Dispute Resolution (ICDR). It has capabilities for conducting arbitrations and ADRs in numerous countries. As COVID-19 set in, the ICDR was one of the first institutions to amend its rules to allow virtual presentations and video hearings. It held over 9,000 virtual events. With COVID-19 restrictions easing now in many cities, the ICDR has now opened hearing rooms in many locations throughout the US. While the number of cases decided in 2021 are not yet available, in January 2022 alone the ICDR resolved 43,205 cases. In 2022, we expect the number of cases decided by ICDR to increase substantially.

The International Court of Arbitration (ICC) is another leading global organization that supervises arbitration and ADR proceedings. It too shut down physical hearings on March 16, 2020, and promulgated rules in 2021 allowing for remote/ virtual hearings. It has since modified its hearing center to provide for in-person, hybrid, and virtual hearings. Despite the COVID-19 virus, 853 new cases were filed in the ICC in 2021, which was a substantial increase over the prior year. In addition, there were 27 cases filed requesting urgent interim orders. We expect that new ICC filings will continue to increase in 2022 and more cases will be decided than during 2021.

The International Centre for Investment Disputes (ICSID) is the leading body for the resolution of investor- state disputes. These disputes involve arbitrations between citizens or corporations of one country that have made economic investments in another country and that other country is alleged to have taken actions that violate the economic rights of such citizens or corporations. According to its annual report, ICSID administered 332 cases during FY 2021, the largest ever administered by ICSID in a single year. We expect increased ICSID activity in 2022 as well.

The Permanent Court of Arbitration at The Hague (The Hague) is the leading arbitration body that conducts disputes between countries. It also conducts investor-state arbitrations. There are a number of such cases that are filed and decided under The Hague. However, in 2021, just one such case was decided. We cannot predict how many such cases will be decided by The Hague in 2022.

In Asia, Hong Kong and Singapore are the main arbitration hubs. Both the Hong Kong International Arbitration Centre (HKIAC) and the Singapore International Arbitration Centre (SIAC) reported an increase in arbitrations during 2020. While neither organization has released the final case numbers for 2021, we expect a similar increase to be reported.

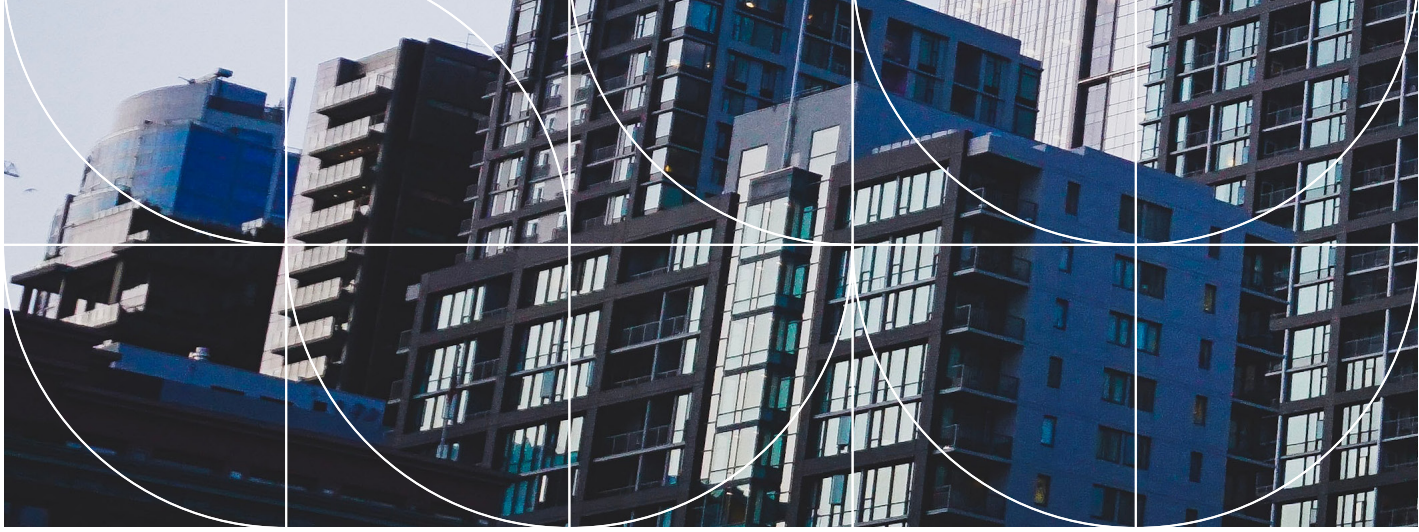
Increased international arbitration activity is likely to continue during 2022. Much of this increase is due to the disruption that COVID-19 continues to bring to international business and supply chains. These disruptions often lead to disputes relating to cost increases and delays to commercial contracts. Of course, non-COVID- related issues, such as intellectual property infringement, will also continue to be driving international arbitrations.

One of the most interesting factors shaping the arbitration market in Hong Kong and Singapore will be each jurisdiction's response to the pandemic during 2022. While Singapore has largely opened up for international travelers, Hong Kong has not and still requires lengthy quarantine stays for those arriving in the territory. In 2021, most arbitrations in both Singapore and Hong Kong were, at least in part, conducted virtually. We may see in 2022 that Singapore moves to more in-person arbitrations, while Hong Kong remains effectively online- only for international participants.

Increased international arbitration activity is likely to continue during 2022. Much of this increase is due to the disruption that COVID-19 continues to bring to international business and supply chains.

In both cases, one can expect the preference for arbitration in large commercial contracts for both Hong Kong and Singapore to continue to grow. The Hong Kong courts remain under a heavy caseload which causes severe delays to cases, an issue not typically faced in arbitration. Moreover, Singapore arbitration often allows legal counsel who may not be Singapore-qualified to be involved. Parties should carefully consider these issues in selecting the appropriate dispute resolution mechanisms contained in new contracts.

In summary, the rivalry between Hong Kong and Singapore in terms of their desire to be Asian arbitration hubs will continue into 2022. We believe that this friendly competition ensures that both jurisdictions will continue to offer excellent arbitration capabilities and will continue to be busy in the coming years.



Key Trends in Commercial Litigation

Real Estate Litigation

— By Mark Johnson and Elizabeth Schrero

This will be a busy year for real estate litigation. Disruption caused by the pandemic continues, and recovery from the pandemic reflects acceleration of pre-pandemic trends.

The rise of e-commerce and changing demands for the use of space will continue. Emerging trends include the growth of some brick and mortar retail operations that began as pandemic online operations, increased use of shared occupancy and multi-uses of premises, and adaptation to new uses of commercial premises. 2022 is also likely to be the year when some residential and commercial development projects and properties that were struggling pre-pandemic, or which benefitted from temporary reprieves or financial assistance, finally will be pushed over the edge.

The landscape continues to change and storm clouds appear on the horizon

We anticipate there will be an uptick in real estate litigation in 2022 due to a variety of factors. Legislatively- imposed moratoriums on enforcement of remedies against distressed tenants and owners, as well as government-sponsored financial assistance, such as the PPP program, functioned as temporary solutions which deferred the consequences of parties' inability to meet their financial obligations. In addition, many parties negotiated short-term solutions with their opposing parties, such as loan forbearance agreements and rent deferral/rent abatement agreements, to avoid litigation and stay afloat. As such short-term remedies and short-term agreements end or prove insufficient, it is likely that the disruptive effect of the pandemic will have an increasingly significant impact on real estate, particularly in the hard-hit retail and hospitality sectors, contributing to the likely increase in lawsuits in 2022.

Commercial landlord-tenant COVID-related disputes

Litigation has worked its way through the courts of many jurisdictions across the country and now informs parties of likely outcomes of future rent disputes based on COVID-related claims.

In 2021, we witnessed many parties and courts invoking and analyzing previously little-regarded lease provisions and old common law excusability doctrines in an effort to resolve disputes stemming from the impact of government shutdown orders on tenants' rent obligations. The results from 2021 have helped to more fully develop the contours of these provisions and defenses, with courts generally tending to skew in favor of landlords, particularly in the office lease context. As for the retail context, the results have been a bit more mixed, with some notable, fact-specific, pro-tenant decisions being issued, resulting in limited relief for tenants.

For contractual provisions, parties focused on *force majeure* clauses (which frequently provide carve-outs for monetary obligations, thereby still obligating tenants to pay rent), co-tenancy provisions (offering relief where other anchor tenants have closed or where, or if, a percentile of the overall leasable area of a shopping center is not occupied for a period of time), operating covenants, casualty provisions, and covenants of quiet enjoyment, the latter two of which have not gained much traction at all for tenants. The most oft-cited common law excusability doctrines were, and continue to be, impracticability, frustration of purpose, and

impossibility. Generally, courts have held parties to the bargains made in their leases and have not excused commercial tenants from their contractual obligation to pay rent during periods when they were forced to close their doors to the public or could not conduct ordinary operations for on-premises business. There have been, however, some notable pro-tenant rulings, which contribute to the uncertain and ever-shifting legal landscape in this area. The key focus is on the actual lease terms, including, in particular, *force majeure* clauses. That is precisely why consultation of specific lease provisions against the prevailing legal landscape is essential for each particular dispute. Notwithstanding the foregoing, where tenants have overreached by seeking reformation or rescission of leases, beyond temporary periods of whole or partial inability to conduct normal business operations, courts have been more steadfast in rejecting such attempts.

Disputes are likely to arise from parties' delay in performing alteration work required under lease agreements or under financing and loan agreements due to labor and supply shortages as well as delays caused by the lock-down periods of 2020 and 2021. Delays in completion of work and development projects will likely spin off other types of claims, including commercial lease disputes arising from parties' failure to comply with work requirements and failure to meet deadlines for delivery of premises or opening for business, as well as co- tenancy disputes (i.e. if a mall anchor tenant is not open, it could trigger rights of other tenants under lease co- tenancy provisions). There also will be related construction loan disputes, guaranty litigation, and mechanic's lien litigation.

Courts have fairly consistently rejected efforts by businesses to recover pandemic-related losses under business interruption or casualty insurance policies because policy language customarily requires a claimant to demonstrate a physical loss.

Construction

Passage of the federal infrastructure bill will spur large-scale projects and developments which are bound to generate disputes ranging from routine construction litigation, to condemnation proceedings and financing disputes, to mechanic's lien litigation.

The pandemic-caused back log of delayed projects will move forward, but there likely will be delay damages and cost overrun disputes. Resolution of these disputes will involve application of the same common law excusability doctrines and contractual *force majeure* clauses that impact commercial landlord-tenant litigation as well as delay damages provisions unique to construction contracts. Whether the parties had the foresight to include pandemic-specific clauses in their construction contracts, or amendments thereto, will go a long way in helping to ascertain where the risk of loss will lie.

Continuing disruption in the real estate market coupled with companies' continued optimism and the proliferation of new opportunities based upon evolving uses and demands for space will also result in increased real estate litigation, since parties will be more likely to again pursue litigation as a tool to achieve desired results.

Key Trends in Commercial Litigation

Real Estate Litigation (cont.)

Purchase and sale agreement and real estate finance disputes

The hot 2021 market for sales and acquisitions likely will generate contract disputes, contract deposit disputes, post-sale claims, and brokerage disputes. We have already seen purchasers' attempts to terminate purchase and sale agreements based upon claims that the economic and business impacts of COVID-19 constitute material changes in value and conditions and thereby entitle them to terminate the agreements.

In addition, changes in borrowers' and occupants' uses of properties may trigger significant changes in lenders' valuations of properties (i.e., a 50% vacant office building likely would be valued differently from an office building with a 10% vacancy rate). This, in turn, may trigger remedies and disputes under loan agreements.

Developing areas of potential liability

Impact of ESG on real estate. ESG (Environmental, Social & Governance) considerations are no longer just lofty and idealistic goals, but rather policies that are integral to the corporate strategies of many entities, including real estate businesses. It has been reported that all major industry groups are formulating data and reporting standards to measure ESG goals and accomplishments.

Public real estate companies are improving transparency and enhancing protection of shareholder value by reporting ESG best practices and may be impacted by public company reporting obligations.

ESG will also impact CRE in the coming years by virtue of required energy reduction and energy transformation costs to reduce energy consumption and shift to sustainable energy. We anticipate these requirements will lead to corporate governance disputes and shareholder disputes arising from alleged inadequate or non-compliant disclosure.

Disclosure obligations and diversity-related claims. Public real estate companies could also face claims arising from inaccurate or incomplete disclosures regarding the impact of COVID-19 on their operations and values.

In addition, we have begun to see some states enact legislation mandating gender diversity on corporate boards, obligating them to comply with board gender diversity disclosure requirements established by the legislation. Failure to do so could expose companies to liability, including for disclosures that contain material misstatements or omissions. Companies also could face shareholder derivative suits alleging breach of fiduciary duties as a result of decisions made concerning board diversity or the lack thereof, or potential harm to their brand.

Climate change. Climate change will continue to significantly impact real estate in certain locations. Government-mandated environmental regulations and modification requirements will also impact valuations and risk assessment decisions by lenders. Shareholder disputes may arise from reporting on compliance and modification requirements as well as related corporate governance decisions. Disputes also will likely arise as to allocation of responsibility to modify properties and regarding rebuilding obligations under commercial lease agreements as well as under loan documents, as lenders seek to protect their collateral.

Cannabis. Legalization of new of cannabis businesses in some jurisdictions will lead to novel disputes with landlords and lenders of properties which have cannabis business tenants, given the continuing illegality of cannabis businesses under federal law and enhanced security, foot-traffic, and related issues associated with such businesses. Landlords can expect challenges around compliance with competing federal law (which criminalizes marijuana possession and use) and local and state ordinances (which prohibit discrimination against, for example, medical marijuana use).

ADA-related litigation. Under the Biden Administration, it appears that there will be heightened enforcement of ADA-related compliance. This in turn likely will generate an increased number of non-compliance claims and actions to compel compliance. The allocation of responsibility for performance/compliance and the costs therefore will likely arise under commercial lease agreements.

Foreclosures and bankruptcy litigation. The retail and hospitality industries were particularly hard hit by the impact of the pandemic. Office leasing, too, has been hard hit due to changing demand for office space. With the end of legislative moratoriums, we anticipate an increased number of mortgage foreclosures and UCC foreclosures on affected hotel properties, as well as guaranty litigation, hotel and retail franchise disputes, and lender liability claims arising from actions taken by parties during the pandemic to defer or forbear from enforcement of remedies.

In addition, shopping mall failures likely will accelerate, with loan foreclosures on mall properties and lease disputes ranging from going-dark litigation, actions to recover rent on vacated spaces, and co-tenancy failures by mall owners, generating other shopping mall lease disputes. This likely will lead to increased bankruptcy filings and work-out related disputes.

As noted above, many landlords, tenants, lenders, and borrowers worked out agreements for at least partial abatements or deferrals of rent or loan obligations in 2020 and 2021. This created a lull in bankruptcy filings in 2021 which likely will end once such temporary relief expires.

Automation and proptech property management and new ownership and management concerns

Potential claims may arise from the shift toward automation and Proptech in development and construction management as well as virtual property management. Novel construction defect claims may arise in relation to construction using 3D printed materials.

Breach of contract and breach of fiduciary duty claims may proliferate in the wake of the tragic Florida condominium collapse to include claims against building owners and management companies which do not undertake proactive measures to prevent similar potential structural disasters. Some jurisdictions, like New York, are adopting legislation requiring periodic structural examination and reporting regarding interior structural components of buildings, as many jurisdictions already have in place with regard to exterior building façades. Claims relating to compliance with such legislative requirements and disputes with professionals and construction parties who perform such services also may arise, as well as claims against property owners and managers which allow deficient structural conditions to persist.

We anticipate litigation involving claims against commercial and residential property owners and managers arising from actions taken or not taken relating to COVID-19 such as potential claims relating to inadequate measures taken to protect against COVID-19 or improper restrictions or obligations imposed relating to COVID-19. Similar claims are anticipated in the context of cooperative and condominium governance disputes.

Conclusion – continued disruption and increased litigation

Seyfarth's 2021 Real Estate Market Sentiment Survey indicated an overwhelming 85% of respondents' believed that 2021 would be a year of opportunity for their real estate companies, as they navigated the fallout from the 2020 recession and adapted to new market demands. Continuing disruption in the real estate market coupled with companies' continued optimism and the proliferation of new opportunities based upon evolving uses and demands for space will also result in increased real estate litigation, since parties will be more likely to again pursue litigation as a tool to achieve desired results.

Key Trends in Commercial Litigation

Securities

— By Paul Ferrillo, Greg Markel, Will Prickett, and Jessica Berk

As the persistent COVID-19 pandemic lingers into 2022, companies (both public and private) and their officers and directors continue to face risk of regulatory and stockholder litigation in the securities law area.

In addition to traditional securities class actions, derivative actions, and investigations that have been commenced at a high level of frequency for most of the past decade (and will continue in 2022 at a slightly reduced level), new risk areas have emerged over the past 18 months and show no sign of abating in 2022. Among those are increasing regulatory enforcement and stockholder litigation arising out of cryptocurrency, "meme" stocks, cyber-security, and Special Purpose Acquisition Companies (SPACs).

Cryptocurrency breaches and fraud are on the rise

There has been a marked increase over the past two years in the number of breaches and fraud claims involving cryptocurrency. The US Securities and Exchange Commission (SEC) has taken a keen interest in increasing both regulation and enforcement actions relating to Crypto. In his October 5, 2021, testimony before the United States House of Representatives Committee on Financial Services, SEC Chair Gary Gensler signaled a strong push for greater SEC oversight: "Currently, we just don't have enough investor protection in crypto finance, issuance, trading, or lending. Frankly, at this time, it's more like the Wild West or the old world of 'buyer beware' that existed before the securities laws were enacted. This asset class is rife with fraud, scams, and abuse in certain applications. We can do better."

One of the key issues to watch in 2022 is the potential for clarity on resolving what category cryptocurrency belongs in; namely, whether it is a security or commodity for purpose of the securities laws. The debate on that issue continues. Leading cryptocurrency executives and investors are pushing for it to be considered a commodity. Commodities generally can be bought and sold on the cash market and are less regulated than securities. The SEC, on the other hand, is seeking more regulatory control over the cryptocurrency market, which would happen if defined as a security. Mr. Gensler has noted there is a "strong case" for classifying cryptocurrency as a security, a stark departure from the view of former SEC Chair Jay Clayton in April 2019.

In November 2021, the SEC rejected the registration of two digital securities offered by American CryptoFed. CryptoFed's filing sought to register the Ducat and another token as "utility tokens" rather than as securities. It remains unclear how successful the SEC will be in litigation over new cryptocurrencies being categorized as securities (or alternatives to securities). However, we can anticipate greater SEC involvement and push for increased regulatory oversight over the purchase and sale of cryptocurrencies in 2022.

Robinhood and other "meme" stocks on the rise in 2022

What began as seemingly innocent posts on Reddit's "WallStreetBets" forum at the start of 2021 resulted in unprecedented price movement and trading frenzy of heavily-shorted stocks. Because of the widespread discussion and hyping of these stocks on many social media sites, the moniker "meme" stock took hold. The price surge of these stocks forced many short-sellers to buy stocks in the companies (which they had bet against) in order to cover their positions and, ironically, this pushed the price of the stocks dramatically higher.

Making this trading volatility worse, Robinhood, the new brokerage app favored by young investors, imposed trading restrictions on these stocks in an effort to raise additional capital to meet collateral requirements.

Despite its troubles, Robinhood itself went public in 2021 and, with its stock value increasing approximately 60 percent in one week, became a "meme" stock in its own right. But increased market price volatility often leads to increased stockholder litigation. The "meme" stock phenomenon is no exception. Dozens of class action suits were filed against Robinhood and others alleging antitrust and securities laws violations, among other claims. In addition, in June 2021, FINRA fined Robinhood $57 million and ordered that the company pay $12.6 million in restitution, plus interest, to thousands of customers harmed between 2016 and 2020.

We anticipate more "meme" stock volatility to continue into 2022. The offer of substantial profit potential, fueled by social media promotion, is likely to be too tempting for retail investors to resist. But such increased spikes in trading and extreme volatility will likely also bring more litigation and regulatory enforcement actions, seeking to curb the risk of market manipulation, fraud and loss to investors.

Cybersecurity risk is in the SEC's crosshairs

Cybersecurity risk is a vital issue for virtually every business. The manner in which those risks are disclosed to investors has become a key focus of the SEC. Recent high profile enforcement actions resulting in fines exceeding $1 million have gotten the attention of issuers and the markets. Given the Biden Administration's statements identifying cybersecurity defenses as a national security priority, we see the SEC moving in parallel in 2022—increasing its scrutiny of risk disclosures and enforcement activity against non-compliant companies.

One of the key issues to watch in 2022 is the potential for clarity on resolving what category cryptocurrency belongs in; namely, whether it is a security or commodity for purpose of the securities laws.

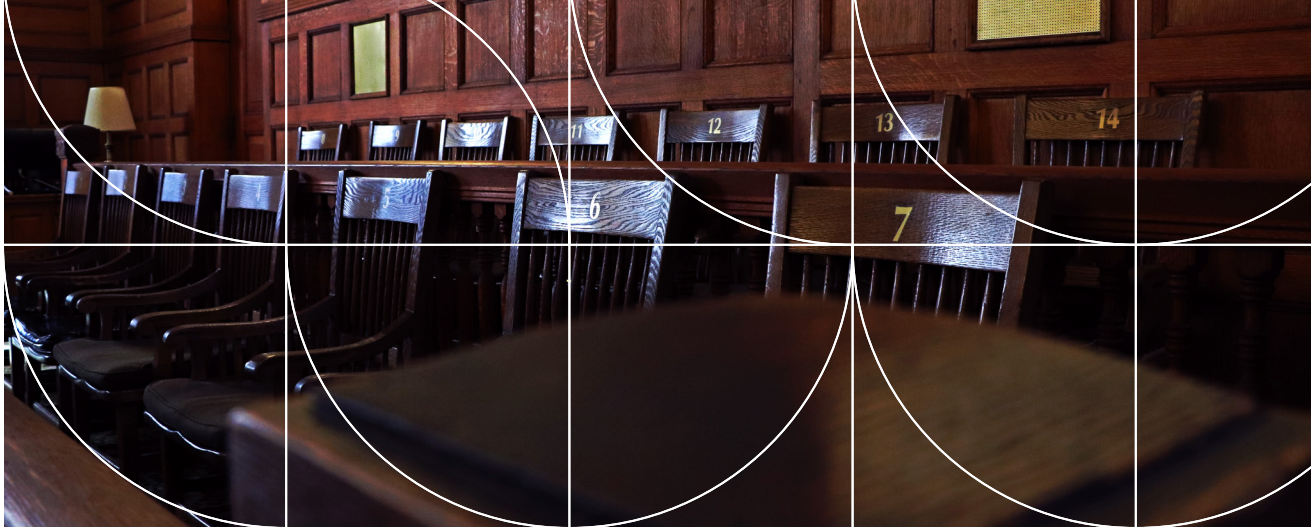
In the summer of 2021, the SEC indicated a change to how it treats cyber threats, signaling a view that more robust (and prompt) disclosure is necessary to protect investors. While public issuers long have been required to disclose "risk factors" in their SEC filings (to warn investors of business risks from competition, natural disasters, supply-chain issues, economic downturns, and the like), cyber risk disclosures have historically been more generic. The increased frequency and severity of cyber attacks over the past several years has led the SEC to conclude that these threats are a clear and present risk to the country's capital markets. This is even where there is no intentional misconduct, and merely negligence in handling a cyber breach. Several recent SEC enforcement actions reflect this SEC view. In 2022, we anticipate seeing more robust and detailed disclosure by issuers of the particular types of cyber threats they face and more issuers opting promptly to disclose breaches that have occurred. However, we still anticipate litigation will be plentiful.

The SECs heightening focus on "SPAC IPOs."

While SPACs have been around for decades, there was an unprecedented increase of these entities formed in 2020 and the first half of 2021. SPACs (publicly traded shell companies formed—and largely controlled by—a "sponsor" management team) became, during that period, a frequent financing device. A key motivation of this increase in SPAC transactions was a desire to reduce regulation of their IPOs by funding the SPAC company before acquiring a business. Once formed, a SPAC raises its own capital through a public offering by the sponsor. It then looks for acquisition candidates, typically established operating companies in a particular industry or sector. If one is found, the SPAC acquires the candidate company (known as the "DE-SPAC transaction) and that company becomes publicly traded. This streamlines the "going public" timeline, and avoids much of the expensive regulatory and underwriting work involved in a traditional IPO.

Commentators and the SEC recently have voiced concerns about this activity, including risks from undisclosed (or poorly disclosed) fees for sponsors, conflicts of interest, and sponsor compensation, as well as the increasing use of celebrity sponsors to hype interest in the transactions. According to Division of Corporation Finance Acting Director John Coates, the SEC is continuing to closely monitor the filings and disclosures by SPACs and their private targets. Specifically, the Division intends to carefully review all SPAC filings, request clear disclosures and provide advice to both registrants and the general public. In addition, dozens of shareholder class actions have been filed in 2021 in the wake of SPAC transactions, most alleging fraud (10b- 5) claims in connection with disclosures about the acquired company's business or prospects. Other shareholder claims have been brought derivatively against sponsors, challenging the structure of the SPAC and the methods of compensating the sponsor.

Going into 2022, there has been a substantial decrease in the initial offering of SPACs. Those ones that are created can expect continued litigation, SEC scrutiny and enforcement activity challenging the adequacy or accuracy of disclosure by these entities to investors. Most important for litigation, there are more than 400 SPACS looking for acquisitions with the clock ticking on deadlines to complete them. The rush to complete acquisitions frequently brings to the fore a conflict between the interest of sponsor of the original SPAC IPO who typically badly want, at any cost, an acquisition and shareholders in the SPAC who want to make only quality acquisition. This conflict will likely result in substantial additional litigation.



Key Trends in Commercial Litigation

Trial Outlook

— By Christopher Robertson

Although it is impossible to know when conditions will permit the resumption of traditional court proceedings, certain aspects of the remote accommodations made by courts to move their dockets forward appear to be here to stay.

We are now close to two years into the disruption caused by COVID-19 on the courts. Yet the question that has not been fully answered is what the civil trial landscape will look like going forward beyond 2022. Most practitioners believe that some aspects of the changes brought on by COVID-19 will remain, such as conducting many routine hearings and conferences remotely. In 2021, we saw the return of in-person jury trials, with judges and court staff making accommodations to the physical layout of courtrooms to protect the participants. We saw jury boxes and courtrooms outfitted for social distancing, with Plexiglass partitions between the judge, jury, witnesses, and counsel. We also saw the federal courts utilize non-courthouse venues to conduct trials, such as military bases and larger federal public buildings. At the state level, we saw state courts utilize various private venues. In Massachusetts, for example, the Trial Court signed licenses with multiple off-site locations to conduct jury trials during the pandemic. These included a private function hall and restaurant, a movie theater, a hotel, and a seasonal resort, among others.

Among other precautions courts are taking include providing supplies of personal protective equipment for distribution to jurors, litigants, witnesses, and others. Hand sanitizing stations are visible and available throughout court facilities. Protective microphone coverings are now standard in many courtrooms. Face shields (as opposed to masks) have been made available, as needed, for witnesses as they testify to assure that facial expressions may be observed and assessed during testimony. In other cases, in order to minimize travel and interactions, courts have held jurors over during trials and conducted jury deliberations in a courtroom adjacent to the courtroom where the trial is being held. The stated goal of the majority of the courts is to bring jury trials back to as close to normal as possible, while continuing to prioritize safety.

As we noted in our outlook for 2021, criminal trials still maintain priority over trials where civil litigants seek a jury trial. For example, in May 2021, the New Jersey Supreme Court authorized the resumption of in-person criminal jury trials, and some in-person civil jury trials, effective on or after June 15, 2021. The court stated that criminal jury trials will be conducted in person and will be the priority, with cases that involve detained defendants continuing to receive the highest priority. The court noted that most civil jury trials at present would continue to be conducted in a virtual format. In Los Angeles, criminal trials maintained priority, followed by juvenile and civil preference cases in which the plaintiff is very sick or elderly. The court noted that juror availability in early 2021 remained a challenge, with less than ten percent of prospective jurors responding to juror summonses (pre-pandemic, the county response rate was around 65%). The court estimated that most civil cases would be continued into 2022.

The stated goal of the majority of the courts is to bring jury trials back to as close to normal as possible, while continuing to prioritize safety.

The significant backlog created by COVID-19 impacted both criminal and civil proceedings, and has required the courts, parties, and their counsel to explore alternatives to in-person proceedings to continue moving cases forward.

While each state's courts and the federal courts have handled the pandemic differently depending on the type of court (trial, appellate, or administrative) and proceeding (criminal, civil, or administrative), some illustrations from certain courts provide a window into what we might see in 2022 and beyond as variants of COVID-19 continue to dominate the headlines and as we confront new health challenges in the future. For example, on November 23, 2021, the Texas Supreme Court issued its Forty-Fifth Emergency Order Regarding the COVID- 19 State of Disaster. That Order provides that courts in Texas may in any case, civil or criminal, even without a participant's consent, allow or require anyone involved in any hearing, deposition, or other proceeding of any kind—including but not limited to a party, attorney, witness, court reporter, grand juror, or petit juror—to participate remotely, such as by teleconference or videoconference. The only limitation on conducting proceedings remotely are in criminal cases where confinement in jail or prison is a potential punishment. In those cases, remote jury proceedings must not be conducted over the objection of the defendant or the prosecutor. In all other cases, remote jury proceedings may not be conducted unless the court has considered on the record or in a written order any objection or motion related to proceeding with the jury proceeding at least seven days before the jury proceeding or as soon as practicable if the objection or motion is made or filed within seven days of the jury proceeding. Likewise, except in a non-binding jury proceeding, a court may not permit or require a petit juror to appear remotely unless the court ensures that all potential and selected petit jurors have access to technology to participate remotely. Alternatively, the Order also allows proceedings to be conducted away from the court's usual location with notice and reasonable public access.

The significant backlog created by COVID-19 impacted both criminal and civil proceedings, and has required the courts, parties, and their counsel to explore alternatives to in-person proceedings to continue moving cases forward. In Georgia, the Fulton County Superior Court implemented a pilot program in civil jury trials to conduct jury selection remotely, followed by an in-person trial. As noted by the Chief Judge, the pilot program was motivated by concern that civil cases were going to continue to face delays because of the crush of demand on criminal dockets. Under the program, prospective jurors received a summons with a Zoom link and instructions about how and when to connect. By moving this process to a remote environment, the court relieved its backlog in civil cases. Additional authority for Georgia state courts to hold video and remote proceedings was extended by the Georgia Supreme Court until the end of June 2022.

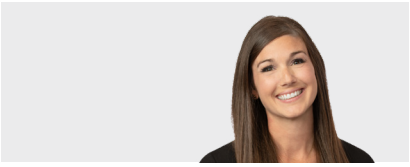
Following the conclusion of two fully remote civil jury trials in Florida in late 2020, Judge Bruce Anderson of the Fourth Judicial Circuit reported to the Florida Supreme Court that fully virtual jury trials are too resource-intensive to be scalable for wholesale implementation across Florida and could not serve as a practical solution for that state's backlog of close to one million cases. In reaching this conclusion, however, Judge Anderson noted that a hybrid jury trial process is a realistic and feasible option for conducting civil jury trials if restrictions imposed by efforts to fight the pandemic persist. As with the pilot program in Georgia, the proposed hybrid process would consist of remote jury selection and an in-person jury trial. Similarly, the Eleventh Judicial Circuit of Florida issued a separate report following a pilot hybrid virtual jury selection and in-person trial which concluded the process did not encounter any serious technical issues.

Numerous additional state and federal trial and appellate courts, including courts in California, Virginia, Illinois, New York, and Washington have overruled objections in civil cases to conducting either aspects of a jury trial or the entire jury trial remotely. Even more courts have concluded that non-jury civil trials may occur remotely in whole or in part. Given the lack of Sixth Amendment concerns in the context of civil matters, these courts have emphasized that the need to move cases forward outweighs any perceived inconveniences or technical issues, while conceding the preference for live testimony if possible to allow jurors to evaluate witness demeanor and credibility in person.

Although it is impossible to know when we will fully emerge from COVID-19 and when conditions will permit the resumption of pre-pandemic, traditional, in-person court proceedings, certain aspects of the remote accommodations made by courts to move their dockets forward appear to be here to stay. The remote accommodations most likely to continue post-pandemic are remote motion hearings and conferences, non-jury evidentiary hearings and bench trials, and possibly remote jury selection followed by in-person civil jury trials. On the other hand, we anticipate that courts and counsel will move back to in-person jury trials as soon as practicable, given some of the challenges to holding such trials remotely experienced during the pandemic.

Authors

Talat Ansari
Partner and National Co-Chair, International Dispute Resolution Group
tansari@seyfarth.com
(212) 218-5539

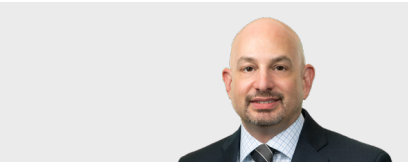


Kristine Argentine
Partner and National Chair, Commercial Consumer Class Action Defense Group
kargentine@seyfarth.com
(312) 460-5332

Jessica Berk
Attorney, Commercial Litigation Practice Group
jberk@seyfarth.com
(617) 946-4853

William Berkowitz
Partner and National Chair, Antitrust & Competition Practice Group
wberkowitz@seyfarth.com
(617) 946-4851

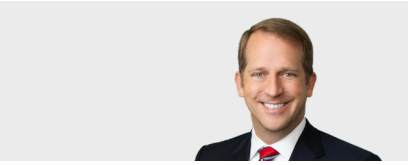
Brandon Bigelow
Partner and National Co-Chair, Antitrust & Competition Practice Group
bbigelow@seyfarth.com
(617) 946-4929



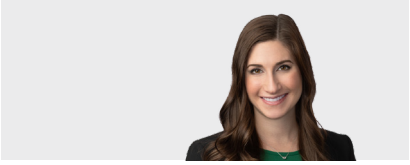
David Bizar
Partner and National Chair, Consumer Financial Services Litigation Practice Group
dbizar@seyfarth.com
(617) 946-4874

Jay Carle
Partner and National Deputy Chair, eDiscovery & Information Governance Practice Group
jcarle@seyfarth.com
(312) 460-6426

Scott Carlson
Partner and National Chair, eDiscovery & Information Governance Practice Group and National Co-Chair, Privacy & Cybersecurity Practice Group
scarlson@seyfarth.com
(312) 460-5946



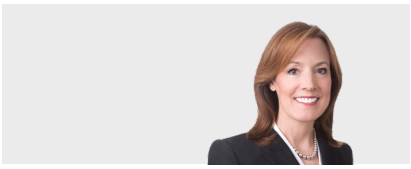
Jesse Coleman
Partner and National Co-Chair, Health Care Group
jcoleman@seyfarth.com
(713) 238-1805



Emily Dorner
Associate, eDiscovery & Information Governance Practice Group
edorner@seyfarth.com
(312) 460-5917

Alison Eggers
Partner, Antitrust & Competition and Franchise & Distribution Practice Groups
aeggers@seyfarth.com
(617) 946-4945

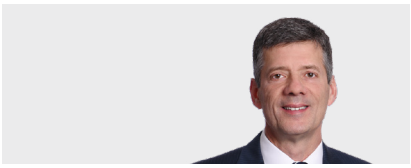
Tonya Esposito
Partner and National Co-Chair, Consumer Financial Services Litigation Practice Group
tesposito@seyfarth.com
(202) 828-5375



Sara Beiro Farabow
Partner and National Chair, International Dispute Resolution Group
sfarabow@seyfarth.com
(202) 828-3591

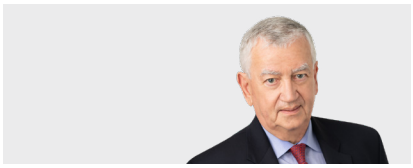
Paul Ferrillo
Partner, Privacy & Cybersecurity Practice Group
pferrillo@seyfarth.com
(212) 218-5558

Bill Hanlon
Partner and National Chair, Bankruptcy & Restructuring Practice Group
whanlon@seyfarth.com
(617) 946-4995



Mark Johnson
Partner and National Chair, Real Estate Litigation Practice Group and Co-Chair, Chicago Litigation Department
majohnson@seyfarth.com
(312) 460-5627

Thomas Locke
Partner and National Chair, Product Liability Practice Group, National Co-Chair, Insurance Coverage, and Chair, Washington, DC Litigation Department
tlocke@seyfarth.com
(202) 828-5376



Greg Markel
Partner and National Co-Chair, Securities and Fiduciary Duty Litigation Practice Group and Chair, New York Litigation Department
gmarkel@seyfarth.com
(212) 218-5579

Esther Slater McDonald
Partner, Commercial Litigation Practice Group
emcdonald@seyfarth.com
(404) 881-5424

Will Prickett
Partner and National Chair, Securities and Fiduciary Duty Litigation Practice Group
wprickett@seyfarth.com
(617) 946-4902

Jason Priebe
Partner and Midwest Regional Manager, eDiscovery & Information Governance Practice Group
jpriebe@seyfarth.com
(312) 460-5608

Christopher Robertson
Partner and National Chair, Whistleblower & Corporate Internal Investigations Practice
crobertson@seyfarth.com
(617) 946-4989

Caleb Schillinger
Partner, Antitrust & Competition Practice Group
cschillinger@seyfarth.com
(617) 946-4944

Elizabeth Schrero
Partner and National Co-Chair, Real Estate Litigation Practice Group
eschrero@seyfarth.com
(212) 218-5522

Authors

John Skelton
Partner and National Chair, Franchise & Distribution Practice Group and Chair, Boston Litigation Department
jskelton@seyfarth.com
(617) 946-4847

Ryan Tilot
Associate, eDiscovery & Information Governance Practice Group
rtilot@seyfarth.com
(312) 460-5958

Owen Wolfe
Associate, Commercial Litigation Practice Group
owolfe@seyfarth.com
(212) 218-3389

Shawn Wood
Partner and National Chair, Commercial Litigation Practice Group
swood@seyfarth.com
(312) 460-5657

Rebecca Woods
Partner and National Co-Chair, Commercial Litigation Practice Group and Chair, Atlanta Litigation Department
rwoods@seyfarth.com
(404) 885-7996

Paul Yovanic
Associate, Workplace Privacy & Biometrics Team
pyovanic@seyfarth.com
(312) 460-5898


EQUAL JUSTICE UNDER LAW

www.seyfarth.com