BakerHostetler

Brief

The Future of Financial Services

Developments in Policy and Regulations, Enforcement, Technology and Litigation

November 2017

On Oct. 6, 2017, BakerHostetler's Financial Services Industry team, in collaboration with the Ohio Bankers League, held its second annual Financial Services Summit in Columbus, Ohio. The speakers included former Consumer Financial Protection Bureau Director Richard Cordray, U.S. Rep. Steve Stivers, R-Ohio, and leading attorneys and financial services executives. The summit included panels on developments in policy and regulation, litigation and enforcement, and the future of blockchain and other financial technologies.

The State of the Industry

Presenter: Jeffrey D. Quayle, *Senior Vice President and General Counsel, Managing Director, Ohio Bankers Benefits Trust*

The latest banking trends

Jeff Quayle began by noting, "The banking industry has a new norm, and so far its rate of return is lower than traditional metrics." He pointed out that average return on assets is rising faster than return on equity, and attributed this trend not to core earnings but rather to conservative regulators. Since the recession, regulators have demanded

additional capital, which results in a return on assets that is higher than the return on equity. In addition, during the recession regulators overestimated losses, and as a result, banks were required to over-reserve. As those reserves have proven to be too high, they are pulled back into earnings. The increase in total earnings somewhat masks the more modest earnings attributable to core banking activities. This "new normal" extends across the industry, Quayle said, but larger banks have a 30 percent higher ROE over community banks, indicating that economies of scale matter.

The key metric to watch is average net interest margin, which has steadily declined over the past 20 years, in part due to "increased competition from a number of sources," Quayle said, adding that the "declining interest rate margin continues to depress core profitability in the banking sector."

Quayle noted that these factors, as well as increased regulatory costs, have led to significant consolidation in the banking industry over the past 30 years; the number of community banks has fallen by more than 10,000. During the same period, the number of regional and large banks has remained consistent. The next driver of consolidation could be challenges in obtaining traditional deposits, Quayle said, which could make it more difficult for banks to fund their loans. "Being able to attract and keep deposits as the Federal Reserve raises interest rates will be a challenge," he said, and those banks that are able to do so efficiently will be the market winners.

In order to help all banks, there are efforts to develop a national consensus on regulatory relief, Quayle noted. While conceding a lack of "public debate on reg relief," he also emphasized the "meaningful discussions among key policymakers in both the U.S. Congress [and] the executive branch." Regulators are trying to address the problem by scaling exams for community banks, easing capital standards and reviving commercial real estate loans. All of that can be done without congressional action, Quayle said, but regulators can only do so much. A healthy banking industry includes creating new charters, he said, pointing out that since 2011, there have been just six new charters created nationally and the Federal Deposit Insurance Corporation (FDIC) has been "extraordinarily conservative" in granting new deposit insurance. Still, he noted that there are currently three groups in Ohio working to form new banks.

Emphasis on cybersecurity

Quayle also addressed the issues of fraud and cyberattacks, which cost both banks and consumers. Cybersecurity will continue to be a vital issue, he said, with banks being "ground zero in this battle."

"Major kudos to banks for being on top of the issue, but the bad guys are getting more aggressive," he said. In 2016, Quayle noted, 13 million people were victims of identity theft, at a cost of $16 billion. The recent breach of credit reporting company Equifax "will go right to the core of how banks access your data," he explained. Old security protocols will no longer be effective, and regulators are looking at how banks of all sizes are managing cyber risk. Quayle recommended that institutions review their cybersecurity plans and, if they have not done so already, establish crisis response plans. He also identified a number of cybersecurity best practices for financial institutions, including ensuring that software patches are routinely applied, using multifactor authentication protocols for access to sensitive systems, and incorporating behavior identification and pattern tracing. Quayle also pointed out that, despite all the technological solutions he mentioned, ongoing training of employees is essential because cyberattacks "come in through your people – one employee or vendor who opens an attachment they shouldn't have."

Internal Investigations Panel

Steven M. Dettelbach, *Partner, BakerHostetler*

F. Thomas Eck IV, *Senior Vice President, Deputy General Counsel, The Huntington National Bank*

Dorothea (Thea) Langsam, *Assistant General Counsel and Vice President, Fifth Third Bank*

Carole Rendon, *Partner, BakerHostetler*

Moderator: Lauren J. Resnick, *Partner, BakerHostetler*

> "Sometimes people are afraid to find things out. Make sure you are not doing that. There is no kind of information but helpful information." – Steven Dettelbach

This panel discussed ways in which financial institutions can proactively manage internal and regulatory investigations to limit risk and drive change within the organization.

Promote a culture of internal reporting to limit risk

One major theme that emerged from the panel is the need for banks to promote a culture that encourages employees to report concerns internally. Thea Langsam described a key difference between how a bank must approach an investigation triggered by an external force such as a subpoena and how it must address one instigated by a whistleblower, which results in an internal investigation. "[W]e want to get to the bottom of it. We're trying to figure out what is the truth," Langsam said, but noted that when the driver is external, the initial focus of the investigation must often be the identification of information and documents to respond to the specific external request. When an investigation is strictly internal, on the other hand, banks "have the luxury to strategize how to approach the issue."

Carole Rendon, a former U.S. attorney, explained how culture really matters in the face of increased whistleblower activity. She said that there are increased incentives for whistleblowers to go to the government, but institutions should encourage their employees to report problems internally first. "Whistleblowers should be blowing the whistle to you, not the government," she said. "If your employees don't think you will listen, or if they have a financial incentive, they will go to the government, and then the bank is in a reactive mode." To avoid that scenario, she suggested that banks make their internal culture as proactive as possible.

Continuing this theme, a panel member added that when confronted with an enforcement action at another institution or an alleged problem in another industry that triggers an investigation, proactive institutions should respond by conducting an internal review for similar vulnerabilities. For example, the panelist noted, financial institutions should use the investigation into Wells Fargo's sales practices as an opportunity to review their own sales practices.

What to do when investigators come knocking

Steven Dettelbach, a former U.S. attorney, explained what government investigators typically expect when an investigation is opened. Investigators "don't expect that you are going to come in on day one and know absolutely everything that occurred and tell them everything," he said. Speaking from his own experience as a seasoned federal prosecutor, Dettelbach added, "I've seen a lot of lawyers make that mistake. They think the first meeting is about resolving the matter, which leads to either over-confessing or pounding the table." He advised that participants be measured and responsive.

The Yates Memo focuses on the involvement of individuals in corporate wrongdoing, and the defendants' counsel are expected to cooperate fully in the investigation of employees and executives. As Dettelbach explained, "This is a challenge to in-house counsel – to set up a structure to take an independent look at individuals who have not done the right thing." Outside counsel can be very useful in these instances, he noted.

Langsam then identified the next steps. She said that when in-house counsel take the lead in an internal investigation, it is good policy for the core team to keep in touch with daily phone calls. She recommended taking two actions at the outset of the investigation response: (1) issuing a litigation hold to instruct custodians who may have documents related to the investigation to preserve those documents and to stop automatic data purges where appropriate, and (2) issuing a direction memo that indicates an investigation is underway, its purpose, and how to prepare for litigation and maintain the attorney-client privilege.

Asked when an institution should bring in outside counsel, a panel member responded, "When you get a call from the DOJ as opposed to a normal examiner."

Define the contours of the attorney-client relationships involved early

It is also important for institutions to identify and clarify the scope of the attorney-client relationships early on, as they are often multilayered. Rendon said that when she is engaged as outside counsel in an investigation, "It is often really necessary to sit down with in-house counsel and figure out who I am reporting to and [whether] other parties need their own counsel. Very clear lines allow you to advise your client on what is in their best interest, which is not always aligned with [the interests of] the company and other parties."

Langsam identified the reporting chain she prefers when dealing with outside counsel, saying it is important that outside counsel treat her – as in-house counsel – as the client. Her client, in turn, is generally the "senior person in the line of business" at the bank. She noted that often it will be worth retaining outside counsel to ensure that the process runs smoothly, especially for smaller in-house legal departments.

Some ideas for managing the mechanics of the investigation

The panelists then moved on to discussing aspects of the interviewing and information-gathering process of an internal investigation. Rendon first addressed the importance of maintaining good records of the investigation, saying, "Putting it in writing helps you remember what you know and how you know it. It allows you to learn from it and make sure it doesn't happen again."

Dettelbach emphasized the importance of investigators asking the right questions to get to the bottom of the issue, adding, "Sometimes people are afraid to find things out. Make sure you are not doing that. There is no kind of information but helpful information."

Whether former employees are included in an investigation is a case-by-case decision, said a panel member. If the Department of Justice wants to talk to that person, then he wants to prepare the former employee and sit in on the interview. Rendon agreed, adding that factors specific to the person also need to be considered. For instance, what were the circumstances of the person's departure – was he or she fired, etc.? How long ago did the person work for the institution? Does this individual now work for a competitor? The institution should evaluate how much can be learned from documents versus how much can be learned only from that person. If the former employee does need to be involved, Rendon suggests working with that person through his or her own outside counsel.

Langsam added that seeking out a former employee could set a precedent that the institution is willing and able to obtain additional information from outside sources. The attorney-client privilege could extend to a former employee, but Langsam warned of the risk that employees could disclose to the government or to the media what they discussed with the institution.

Other important considerations

When remediation is required after an investigation, Dettelbach said, institutions must determine how to change, rethink training and hold people accountable in the future. He also noted that often this is easier for large institutions that have funds to spend on compliance. A panel member added that regulators expect that the bank will make the consumer whole. To do so, the institution may need to "break down the silos and have an integrated response."

Rendon added that institutions should also have a media strategy for investigations. "Even if it never becomes public, proactive planning helps you make the best decisions," she said. It is very important to inform customers about the issues, and about how they are being corrected and prevented to ensure the customers continue doing business with the institution. The institution may resolve the issues, but the plan could all fall apart if no one is coming back.

Dettelbach concluded by noting that the financial institution's board should be fully briefed and included in any internal investigation. "Engage very early. The biggest mistake is putting it off," he said. "Err on the side of inclusion." He also warned that it is a mistake to "confront people late in the process with things they think are already decided."

Finserv Litigation Panel

Mark T. Freeman, *Associate General Counsel, KeyCorp*

Jennifer Mountcastle, *Associate General Counsel and Vice President, The Huntington National Bank*

Anthony M. Sharett, *Marketing and Emerging Businesses Legal Leader, Nationwide*

Daniel R. Warren, *Partner, BakerHostetler*

Moderator: Joseph E. Ezzie, *Partner, BakerHostetler*

> "Make sure that outside counsel and e-discovery vendors meet certain cybersecurity requirements. We survey outside firms regarding protocols and systems." – Mark Freeman

The panelists responded to several questions and discussed recurring issues facing financial institutions brought about by litigation.

What are the emerging trends in the world of financial services litigation?

Mark Freeman first discussed how the use of consumer arbitration coupled with waivers on consumer class actions has helped financial institutions avoid significant costs when handling consumer disputes. However, "There is no 'one size fits all' answer," Freeman said. "To be beneficial and fair, it takes a lot of thought to draft an arbitration provision."

A panel member reported a rise in claims brought by visually impaired plaintiffs under the Americans with Disabilities Act (ADA) due to alleged inaccessibility of companies' websites. While retailers are currently facing the majority of these suits, the panelist warned that financial services institutions should expect an increase in this type of litigation as well. The panelist noted that the ADA does not directly address the accessibility of websites, the Department of Justice has not yet provided regulatory guidance on the issue, and case law is mixed. As a starting point, financial institutions need to ask themselves, "What is the state of our website's accessibility?"

Next, Anthony Sharett identified that the industry is experiencing an increase of third-party vendor litigation, specifically in the financial technology (Fintech) space. He explained that these suits typically focus on the language in service level agreements that measures the performance of the third-party vendor. However, he has noticed that more

of these vendors are taking their cases to trial – an effect he attributes to the proliferation of the Fintech industry. In order to minimize the risk of third-party vendor litigation, moderator Joseph Ezzie suggested companies establish third-party contract review groups to review and negotiate contract language within service level agreements.

Daniel Warren finished off the issue by discussing how financial institutions today are being exposed to a wider variety of lawsuits than in previous decades. He specifically noted the rapid evolution of privacy litigation, as well as a rise in litigation stemming from changes financial institutions make to their "internal workings" and their relationships with third-party vendors. As a result of this diverse landscape of litigation, Warren has observed a concurrent increase in risk management programs within financial institutions. "There have been great advances in handling litigation risk," he said.

Convincing business clients that contract language makes a huge difference

Business clients do not always understand how crucial contract language can be. A panel member stated, "The design of arbitration clauses can be very problematic." The panelist continued, "More often than not, these clauses are written by someone who has never participated in arbitration. Business clients need to understand the need to get the in-house or outside litigation counsel involved in developing the clause."

What is the bank examiner's privilege, and how does it work?

The panelist's discussion then moved to the bank examiner's privilege and its application to financial services litigation. Freeman explained that the privilege protects confidential supervisory information (CSI), which can include communications between financial institutions and regulators, data collected by the regulators as part of their enforcement responsibilities and examination reports. Regulators have the initial burden of establishing that the privilege applies, but the party seeking the information is given the opportunity to contest the application of the privilege. Freeman believes that most CSI claims are uncontroversial and regulators are generally protective of information that constitutes CSI. There is the risk of waiver of the privilege if a regulator does not actively protect it. However, what constitutes a waiver is uncertain, as there isn't a lot of case law that has touched on this topic.

Freeman recommends that when plaintiffs request CSI, financial institutions direct them to the regulators, who own the privilege. Sharett added that in a federal criminal matter, financial institutions may be inclined to provide CSI to the Department of Justice, but that it is imperative companies get the permission of the respective regulators before doing so.

The explosion of electronic discovery and Rule 26's proportionality rule

Ezzie next asked the panelists about the cost and work associated with e-discovery, particularly in light of the fact that less than 1 percent of civil matters ever make it to trial.

Warren responded, "Because so few cases go to trial, young lawyers tend not to understand cases as well as attorneys who have experience taking cases to trial." He added that due to the sheer amount of discovery produced, the initial document review of cases, which is not usually done by the first- or second-chair trial attorneys, is extremely crucial. Warren also noted that courts are starting to manage discovery differently by cutting down on the quantity and duration of depositions. But these changes are having good effects, he added, because they prevent counsel from "going down every rabbit hole" and cause them to prepare the depositions, and the case as a whole, much differently. "When depositions are limited like this by the court, counsel treat them more like trial depositions and they end up being more effective and much cheaper," he said.

Sharett commented on ways to cope with the significant demands of electronic discovery, explaining, "Nationwide has an in-house discovery unit that works nationally regarding ESI. It's a great partnership." The bank's in-house counsel collaborate with the discovery management unit from the beginning of a matter.

When asked about the effectiveness of the proportionality requirement of Rule 26 of the Federal Rules of Civil Procedure, Warren responded, "Proportionality rules are essential, but it's a little too early to see how it's working in practice." Sharett added that outside counsel are more successful in cutting down on excessive discovery when they focus on the monetary burden the requests have placed on the producing financial institution.

A panel member closed out this discussion by commenting that it is crucial for companies to capture and retain the right amount of documentation. In light of overlapping litigation hold obligations, keeping documents longer than necessary for business purposes makes it challenging to get rid of those documents in the future. Good document retention policies, particularly those related to emails, are the "best medicine."

Managing the litigation and outside counsel

The in-house counsel panelists then discussed how their respective teams deal with litigation internally and manage the outside counsel they hire. Sharett said Nationwide's internal litigation group utilizes early case assessments from outside counsel to identify trends in litigation and keep outside counsel accountable.

Freeman noted that KeyCorp has a similar in-house litigation group. Deciding on which outside counsel to use depends on the strengths of the respective firms and looking at the nature and size of the particular case. His internal team tracks the litigation and devotes significant resources to case management because of the regulatory environment surrounding the financial services industry. He further emphasized the importance of cybersecurity when involving outside counsel, stating, "Make sure that outside counsel and e-discovery vendors meet certain cybersecurity requirements. We survey outside firms regarding protocols and systems."

Fintech/Blockchain Panel

Pat Berarducci, *Deputy General Counsel and Full-Stack Software Developer, ConsenSys*

John J. Harrington, *Partner, BakerHostetler*

Laura E. Jehl, *Partner, BakerHostetler*

Casey Kuhlman, *CEO, Monax*

Moderator: Robert Craig, *Chief Information Officer, BakerHostetler*

> "The idea that blockchain will save the world may not be true, but it will change the world." – Robert Craig

This panel discussed the importance of blockchain technology, its current and potential future applications, and the challenges it poses.

The importance of blockchain technology

Blockchain technology, Pat Berarducci explained, is a "disruptive technology" analogous to the printing press, the computer and the internet. All of these innovations simplified and expanded human communications. Blockchain technology does this by "simplifying and expanding human agreements," Berarducci said, "especially with people we don't know and we don't trust." For example, parties can enter into "smart contracts" that are executed in automated code in a blockchain that anyone can inspect and verify. In addition to smart contracts, application of blockchain technology also extends to cryptocurrencies and self-sovereign identities.

Cryptocurrencies and efforts to regulate them

Cryptocurrency, with a capitalization of upward of $200 billion, is among the most important applications of blockchain technology. The first cryptocurrency, bitcoin, was inspired by the 2008 financial crisis and created a year later.

Bob Craig explained that although bitcoin is the most well-known application, is it not the only one: Thousands of others are being developed across a variety of industries. In fact, dozens of blockchain consortia have been formed by industry groups to better understand and benefit from this technology. Although the financial services industry leads the way, others such as accounting, insurance and healthcare are taking interest and formulating strategies.

Companies can leverage cryptocurrencies to jump-start new products, services and businesses by selling "tokens" on the Ethereum blockchain, Berarducci added. Tokens are programmable, digital assets that can represent and function as just about anything, so the possibilities are endless. Some people refer to sales of these tokens as initial coin offerings, or ICOs. These sales present new regulatory problems.

John Harrington, a former Securities and Exchange Commission (SEC) official, noted that as a technology with significant implications for securities, capital raising and investor protection, blockchain is on the SEC's radar. Depending on their characteristics, some tokens may qualify as securities under federal securities laws. Earlier this year, for example, the SEC issued an investigative report on a virtual organization called "The DAO," which operates a tokenized venture fund. The SEC determined that the DAO tokens qualified as an "investment contract," because they constituted investments in a common enterprise fund with the expectation of profits from the efforts of others. The SEC concluded that, as investment contracts, the DAO tokens were securities and should have been registered prior to sale. The SEC has signaled that other tokens satisfying this test will likewise implicate the federal securities laws and require registration.

In addition to the SEC, states also are in the process of regulating cryptocurrency. For example, some are developing laws about how to treat cryptocurrency for tax purposes, money transmitter regulation and securities registration.

The rise of the self-sovereign identity

Laura Jehl explained how blockchain makes it possible to implement a self-sovereign identity – a portable identity that is not dependent upon any particular company or government. Currently, internet users interact with innumerable organizations, using a separate identity for each one, with passwords, security questions, etc. But blockchain can allow users to recognize each other as secure digital individuals, an approach that can provide verifiable identities for huge numbers of people who do not have documented identities, such as refugees. Underscoring the potential importance of this application is the United Nations' target of providing everyone in the world with a verifiable identity by 2030.

Blockchain and smart contracts

Casey Kuhlman's company, Monax, is on the cutting edge of combining blockchain and smart contracts with real-world complexity. Kuhlman's company is focused on using blockchain to automate transaction flows in low-trust environments. "Smart contracts are neither smart nor contracts," he explained. "They should be called 'small scripts,' an order event log kept in sync across computers." Through a smart contract, agreements can be formulated, verified and tracked in blockchain. He conceded, however, that "[t]he paper contract has the ability to cover more complexity than computers can. Good or bad, that is reality."

Sophisticated business processes can also be built into products and then commoditized, he said. Such products could be used, for example, to lower the cost of regulatory compliance for smaller banks. This application could replace some of the duties of a company's legal counsel. Still, there are many uncertainties surrounding blockchain, including how it can be leveraged by average businesses. Kuhlman noted that blockchain technology can be run across many systems, potentially lowering coordination costs, but its operational risks are unclear.

Bad actors' use of blockchain

Jehl addressed the privacy and security implications of blockchain, noting that criminals can steal money from blockchain transactions or use cryptocurrency to receive money anonymously. In one notable digital currency exchange hack, $70 million worth of bitcoin was stolen. "While the transactions were transparent," she said, "the bitcoin was still gone. Anything connected to the internet can be hacked." The anonymity of digital currency has made it popular with cybercriminals, particularly those who deploy ransomware to lock up computer systems and then encourage victims to pay the ransom with bitcoin or other digital currencies. "Anonymity and compliance are fundamentally in opposition," Jehl said. "Bad actors like anonymity more than good actors do." Fortunately, law enforcement has gotten better at tracing transactions and catching cybercriminals.

Government Policy and Regulations

Representative Steve Stivers *(R-Ohio)*

The Hon. Michael A. Ferguson, *Senior Advisor, BakerHostetler*

"Consumer protection is best done as an integrated piece of overall regulation." – U.S. Rep. Steve Stivers

In an informal "fireside chat" format, U.S. Rep. Steve Stivers talked with the Hon. Michael Ferguson, leader of BakerHostetler's federal policy team and a former member of the U.S. House of Representatives. Before entering the House, where he is serving his fourth term on the Financial Services Committee, Stivers worked in the Ohio banking industry. His time in the private sector showed him the burdens that regulations can place on ordinary citizens. "We have to be clear and effective in regulations and legislation," he said.

Stivers noted the increased regulatory burden on individuals and small businesses resulting from the 2008 financial crisis. "I think the pendulum has swung too far in the regulatory direction," he said. "The unspoken thing we have done is deny credit to people with credit scores below 600, 700. And we wonder why so many people are unbanked." Instead, government should use its "precious regulatory capital" on what is most essential, and should do so effectively. "Consumer protection is best done as an integrated piece of overall regulation," he added.

SEC Chairman Jay Clayton recently testified before the Financial Services Committee about the need for the government to protect data for which it is the custodian; the efficiency of the markets structure; and the Volcker Rule, which prohibits banks from conducting certain investment activities with their own accounts and limits ownership of hedge funds and private equity funds. Stivers noted that possible changes to the rule have been discussed under the Trump administration and added that he thinks Clayton "is doing a great job and moving in the right direction."

Stivers also emphasized the importance of cybersecurity in light of the recent Equifax breach. He proposed a cross-jurisdictional task force to address the increasing risk of breaches. "It's only getting worse, and if we do nothing, we will be buried under breaches and every American's data will be gone," he said. Stivers also identified cyber insurance as a way to reduce the impact of a breach; costs would be based on the amount of risk in which the company engages, much like workers' compensation insurance.

Stivers said he has met with Federal Reserve officials to discuss ways to relieve the regulatory burden on smaller banks. He called for expanding examination cycles for well-run banks, and for consistency in applying regulations, noting that field examiners do not always interpret regulations the same way across the board. "There is overthinking going on," he said. "We need to get people understanding that it wastes time [and] hurts our financial system and economic growth. I'm hopeful we can turn that around."

In closing, Stivers offered his view of how the Senate Banking Committee, chaired by Sen. Mike Crapo, R-Idaho, with Sen. Sherrod Brown, D-Ohio, as the ranking Democrat, might address regulatory reform in the banking industry. He noted that the Republicans were working well with their Democrat counterparts, and was optimistic that regulatory reform could be passed given the committee's "very bipartisan environment."

Conclusion

The panels at this year's event, The Future of Financial Services, provided a practical overview and insights on key challenges facing the financial services industry from the perspectives of many stakeholders, including in-house counsel, outside counsel, government officials and industry experts. For additional information on any of the subjects discussed above, please contact one of these BakerHostetler attorneys.

Financial Services Industry Key Contact

Brett A. Wall
T +1.216.861.7597
bwall@bakerlaw.com

Additional Contacts

Robert Craig
T +1.216.430.3030
rcraig@bakerlaw.com
**not an attorney*

Steven M. Dettelbach
Cleveland
T +1.216.861.7177
Washington, D.C.
T +1.202.861.1621
sdettelbach@bakerlaw.com

Joseph E. Ezzie
T +1.614.462.4758
jezzie@bakerlaw.com

Michael A. Ferguson
T +1.202.861.1663
mferguson@bakerlaw.com
**not an attorney*

John J. Harrington
T +1.216.861.6697
jharrington@bakerlaw.com

Laura E. Jehl
T +1.202.861.1588
ljehl@bakerlaw.com

Carole S. Rendon
T +1.216.861.7420
crendon@bakerlaw.com

Lauren J. Resnick
T +1.212.589.4241
lresnick@bakerlaw.com

Daniel R. Warren
Cleveland
T +1.216.861.7145
Chicago
T +1.312.416.8179
dwarren@bakerlaw.com

bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.